NAS System

User's Manual

Revision 1.0

Table of Contents

PART I Hardware Components and RAID Controller 7

Chapter 1 Introduction 8

1.1 Key Features 9
1.2 Technical Specifications 10
1.3 RAID Concepts 13
1.4 Array Definition 16
1.4.1 Drive Group 16
1.4.2 Virtual Drive 16

Chapter 2 Getting Started 17

2.1 Packaging, Shipment and Delivery 17
2.2 Unpacking the NAS System 17
2.3 Identifying Parts of the NAS System 18
2.3.1 Front View 18
2.3.2 Rear View 19
2.3.3 LCD Display Panel 20
2.3.3.2 LCD Front Panel Function Keys 20
2.4 Drive Carrier Module 22
2.4.1 Disk Drive Status Indicators 22
2.4.2 Lock Indicator 22
2.5 Installing Hard Drives 23
2.6 Preparing the System 24
2.7 Powering On 24

Chapter 3 RAID Configuration and Management 25

3.1 WebBIOS Configuration Utility 25
3.1.1 Starting the WebBIOS Configuration Utility 25
3.1.2 WebBIOS CU Main Screen Options 26
3.2 Configuring RAID Drive Groups and Virtual Drives 28
3.2.1 Using Auto Configuration 30
3.2.2 Using Manual Configuration: Creating RAID 5 Virtual Drives 31
3.3 Creating Global Hot Spare 39
3.4 Restarting the Controller 41

PART II proNAS System 43

Chapter 4 Introduction 44

4.1 proNAS Key Components 44

4.2 Installation and Configuration Phases....45
4.3 Setting proNAS IP Address and Connecting to NAS Management GUI....46
4.4 Basic Steps in Creating Raid Set Using Raid Manager....49
4.5 Raid Manager....52
4.5.1 Using Raid Manager....52
4.5.2 Disk List....54
4.5.2.1 Create Hot Spare Disk....55
4.5.2.2 Delete Hot Spare....57
4.5.2.3 Alert Off / Alert On....59
4.5.3 Raid Set List....60
4.5.3.1 Create Raid Set....61
4.5.3.2 Edit Raid Set....64
4.5.3.3 Delete Raid Set....67

Chapter 5 proNAS Manager....69

5.1 Volume Manager....70
5.1.1 Volume Group Management....71
5.1.1.1 Create the proNASVG Volume Group....71
5.1.1.2 Creating another Volume Group....75
5.1.1.3 Reset and Remove Volume Group....79
5.1.2 Logical Volume Configuration....81
5.1.2.1 Create new Logical Volume....81
5.1.2.2 Extending Logical Volume Size....84
5.1.3 Volume Snapshot....86
5.1.3.1 Create Snapshots in Logical Volumes....87
5.1.3.1.1 Create Snapshots Manually....87
5.1.3.1.2 Create Snapshots Based from Schedule....90
5.1.3.2 Creating Snapshots in FC Target Manager....94
5.1.3.3 Creating Snapshots in iSCSI Target Manager....96
5.1.3.4 Delete Snapshots....98
5.1.4 Volume Replication....100
5.1.4.1 Replication Configuration....101
5.1.4.2 Checking the Status of Replication....107
5.1.4.3 Extending Logical Volume under Replication....108
5.2 FC Target Manager....109
5.2.1 Target List....110
5.2.1.1 Port Config....111
5.2.2 Volume List....112
5.2.3 Secure List....114
5.2.4 Connecting Host to FC Target Volume....117

5.3 iSCSI Target Manager 118
5.3.1 Target List 119
5.3.2 Volume List 120
5.3.3 Secure List 122
5.3.4 Connecting Host to iSCSI Target Volume 123
5.4 Network Manager 124
5.4.1 Network Setting and Trunking 124
5.4.1.1 Configure Network Adapter Trunking 126
5.4.1.2 Cancel Trunking 129
5.4.2 Internet Gateway 131
5.4.3 Network Policy 132
5.4.4 SNMP 134
5.4.5 Network Test 135
5.5 Account Manager 136
5.5.1 External Accounts Integration (Domain Account Authentication) 136
5.5.1.1 Windows Authentication 136
5.5.1.2 Sample Steps to Join the NAS to Windows AD Domain: 138
5.5.1.3 NIS Authentication 140
5.5.1.4 Sample Steps to Join NIS Domain: 140
5.5.1.5 LDAP Authentication 141
5.5.1.6 Sample Steps to Setup LDAP: 142
5.5.2 Local Account and Group Management 143
5.6 Share Manager 153
5.6.1 Share Management 155
5.6.1.1 Creating a New Share 155
5.6.1.2 Applying ACL 156
5.6.1.3 Modifying a Share 157
5.6.1.4 Deleting a Share 157
5.6.2 Properties Setting 158
5.6.2.1 Steps to Make a Share Folder a Public Folder Accessible to All Users: 159
5.6.3 Protocol Setting 160
5.6.3.1 CIFS 160
5.6.3.2 NFS 161
5.6.3.3 AppleTalk 162
5.6.3.4 How to Setup Time Machine 163
5.6.3.5 How to Use WORM 169
5.6.3.6 How to Use WebDAV 175
5.6.4 Privilege (Permission Setting) 185
5.6.4.1 Group 185
5.6.4.2 Account 187

5.6.4.3 IP Address....189
5.6.5 Rsync....191
5.6.5.1 How to Setup Rsync....196
5.6.6 Duplication....203
5.6.7 Default Share....208
5.6.8 Recycle Bin....209
5.6.9 Audit....212
5.7 System Manager....215
5.7.1 Information tab....216
5.7.2 Upgrade tab....217
5.7.3 Report tab....219
5.7.4 Time tab....220
5.7.5 Serial Ports tab....221
5.7.6 Power tab....223
5.7.7 Reboot tab....224
5.7.8 Service tab....225
5.7.9 Status tab....228
5.7.10 MRTG tab....229
5.8 Backup Manager....230
5.8.1 proNAS Configuration Backup....231
5.8.2 Configure Backup Plan....232
5.8.3 Tape Control....238
5.8.3.1 Backup and Restore Using Tape....239
5.9 Log Manager....258
5.10 Event Manager....259
5.10.1 E-Mail Setting....259
5.10.2 Event Setting....260

Chapter 6 File Manager....263

6.1 Introduction to File Manager....263
6.2 Logon to File Manager....265
6.3 Directory and Upload Function....266
6.4 User Access Right and Group Access Right....268
6.5 Change Password and Logout....268

Chapter 7 proBackup....269

7.1 Introduction to proBackup....269
7.2 Administrator Logon....269
7.3 Create Backup Plan....272
7.4 Restore Backup....278
7.5 Account Detail....279

Chapter 8 proNAS HA (Optional Function) 280

8.1 Introduction to proNAS HA 280
8.2 Getting Started with proNAS HA 281
8.2.1 Hardware Aspect 282
8.2.2 Procedure for Setting Up proNAS HA 283
8.3 ProNAS HA Properties 292
8.4 Extending a Logical Volume in HA 293
8.5 Clear All HA Configuration 294
8.6 License Registration 297
8.7 Event Log Properties 298

PART I Hardware Components and RAID Controller

Chapter 1 Introduction

The NAS System

Companies are looking for cost-effective storage solutions which can offer the high performance, high scalability and reliability. As the number of users and the amount of data grows, Network Attached Storage is becoming a critical technology and the need for an optimized solution is becoming an important requirement. Proware delivers the EPICA NAS subsystem together with the proNAS management solution, proNAS High-Availability and proBackup client backup solution to provide businesses with the most flexible, scalable, securable and manageable NAS environment. It helps to control the total cost of ownership for data management.

The EN-3166JS6H-SQX is an 6Gb SAS/SATA NAS Subsystem with proNAS 1.3 operating system. It enhances system availability, and manages complex storage environments easily. For improving business productivity and minimizing business risks, EN-3166JS6H-SQX provides a volume replication and a volume snapshot function. It is also a full featured data protection system supporting RAID levels 0, 1, 5, 6, 10, 50 and 60. It supports hot spares, automatic hot rebuild and online capacity expansion within the enclosure.

1.1 Key Features

- Configurable to 19" rack-mountable 3U chassis
- INTEL Nehalem based
- Supports up to Sixteen (16) 1" hot-swappable 6Gb SAS/SATA hard drives
- Supports Tape/DAT backup/restore (Option)
- Supports RAID levels 0, 1, 5, 6, 10, 50 and 60
- Smart-function LCD panel for ENC status
- Supports hot spare, automatic hot rebuild and online expansion file system
- Allows online capacity expansion within the enclosure
- Two Gigabit Ethernet ports, Support optional 10 Gigabit Ethernet
- 64 bit Linux-based embedded system
- Centralization of Data and Storage Management
- Using Market-Leading Java Technology
- Latest volume snapshot technology
- Apply volume replication to enhance data protection
- Support logical volume over 2TB (Maximum 8 Exabytes)
- Support iSCSI Target and iSCSI Target trunking
- Support SFTP files transmission
- Support SNMP remote monitor system with hardware status
- Support Ethernet trunking to 8 ports
- Data Backup via backup plan and scheduling
- Enhance system configuration backup
- Local and external account management, support large account import
- Share management and permission (support ACL setting)
- Support E-mail notification and system log information
- Multi application support via proFamily

1.2 Technical Specifications

Hardware Specification
Intel Quad Core Xeon 3.1GHz Processor
Cache Memory：2GB DDR3 ECC SDRAM up to 32GB
Three Gigabit Ethernet ports (option for 10Gigabit Ethernet)
Supports 16 SAS2 / SATA3 hard drives
Expansion PCI slot for H/W upgrade
Environmental monitoring unit
Two(2) 460W high efficiency hot-swap power supplies with PFC
Real time drive activity and status indicators
Power requirements
AC 100V ~ 240V Full range
10A ~ 5A, 47Hz ~ 63Hz
RAID Controller
800MHz RAID-On-Chip storage processor
RAID level RAID 0, 1, 5, 6, 10, 50, 60
Supports 512MB DDRII cache memory
Supports hot spare and automatic hot rebuild
Allows online capacity expansion within the enclosure
Local audible event notification alarm
Storage Management
Volume Management (Support XFS, ext3 & ext4 file system)
Disk usage statistics
Hot spare capability
iSCSI Target Manager: Support LUN Mapping / Initiator filter
FC Target Manager: Support LUN Mapping
General
File Server Independent
Multiple language support
Support UPS management
Support AES 256bit logical volume encryption

System Management
Automatic IP address configuration
Self-contained unit - no extras needed
Management through Web browser
Flash upgradeable unit
SNMP / MRTG management and notification
Fail-free online firmware upgrade
Unicode support
Multi-node Management GUI
proNAS Configuration Backup
Central Management
Networking
Supports NIC / Trunking / load balance / fail over / 802.3ad
DHCP Server / DHCP Client
WINS Server
Internet gateway
Protocols
TCP/IP, SMB/CIFS, NFS, SNMP, FTP/SFTP/FXP, HTTP, HTTPS, Telnet, SSH, AFP ,(Novell by TCP/IP, WebDAV)
Client Operating Systems Support
Microsoft® Windows® 98/ ME/ NT/ 2000 / XP / 2003 / Vista /2008
Unix / Linux
Mac OS
Authentication
Local User Account/Group
Microsoft NT Domain Controller (PDC)
Microsoft Active Directory Authentication (ADS)
Network Information Service (NIS)
Support batch creating users/Group
User quota management
Share level security
File level security

User ID security for NFS
Recycle bin (Samba)
Audit file access (Samba)
Write once read many (WORM)
Block Storage
iSCSI Target Support
Fiber Target Support (optional)
Data Backup / Restore
Symantec BackupExec Agent (by additional installation)
Scheduling Multi-Snapshot (Support snapshot of iSCSI & FC)
Replication (Remote RealTime Data mirror)
proNAS High-Availability (optional)
Scheduling Duplication
Scheduling Rsync Replication
proBackup from client to NAS
Support NetVaultR backup Client (by additional installation)
Support CA ARCserve (by additional installation)
Support CDP Server (by additional installation)
Support Mac Time machine
Physical Dimension
133(H) x 482(W) x 730(D) mm

Specifications are subject to change without notice.

1.3 RAID Concepts

RAID Fundamentals

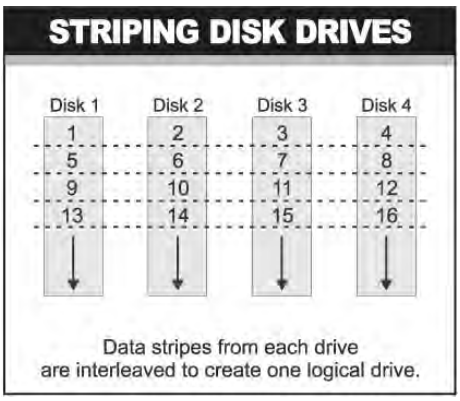
The basic idea of RAID (Redundant Array of Independent Disks) is to combine multiple inexpensive disk drives into an array of disk drives to obtain performance, capacity and reliability that exceeds that of a single large drive. The array of drives appears to the host computer as a single logical drive.

Five types of array architectures, RAID 1 through RAID 5, were originally defined; each provides disk fault-tolerance with different compromises in features and performance. In addition to these five redundant array architectures, it has become popular to refer to a non-redundant array of disk drives as a RAID 0 arrays.

Disk Striping

Fundamental to RAID technology is striping. This is a method of combining multiple drives into one logical storage unit. Striping partitions the storage space of each drive into stripes, which can be as small as one sector (512 bytes) or as large as several megabytes. These stripes are then interleaved in a rotating sequence, so that the combined space is composed alternately of stripes from each drive. The specific type of operating environment determines whether large or small stripes should be used.

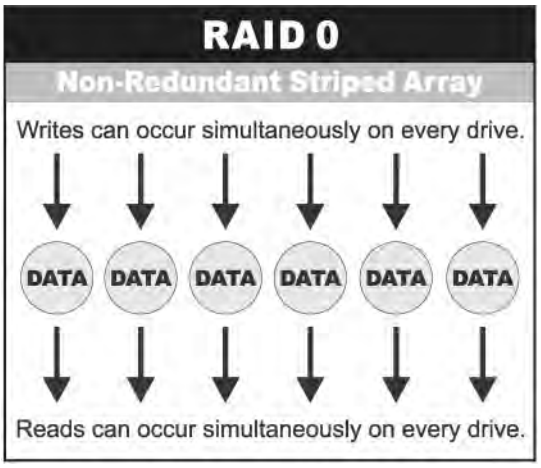
Most operating systems today support concurrent disk I/O operations across multiple drives. However, in order to maximize throughput for the disk subsystem, the I/O load must be balanced across all the drives so that each drive can be kept busy as much as possible. In a multiple drive system without striping, the disk I/O load is never perfectly balanced. Some drives will contain data files that are frequently accessed and some drives will rarely be accessed.



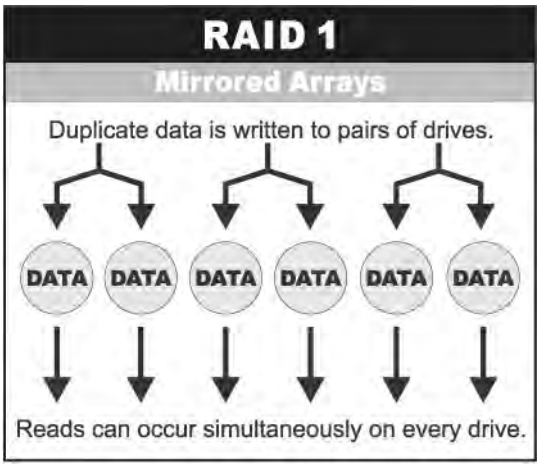
By striping the drives in the array with stripes large enough so that each record falls entirely within one stripe, most records can be evenly distributed across all drives. This keeps all drives in the array busy during heavy load situations. This situation allows all drives to work concurrently on different I/O operations, and thus maximize the number of simultaneous I/O operations that can be performed by the array.

Definition of RAID Levels

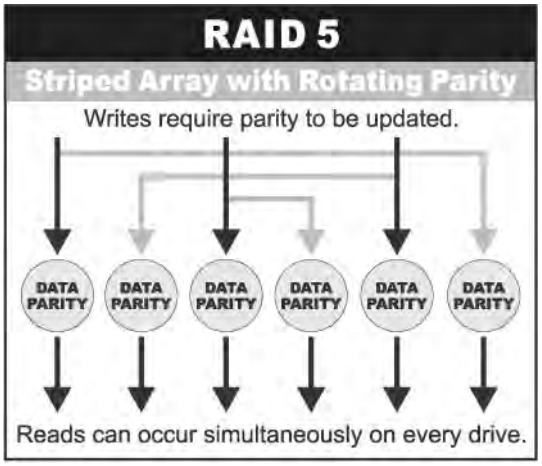
RAID 0 is typically defined as a group of striped disk drives without parity or data redundancy. RAID 0 arrays can be configured with large stripes for multi-user environments or small stripes for single-user systems that access long sequential records. RAID 0 arrays deliver the best data storage efficiency and performance of any array type. The disadvantage is that if one drive in a RAID 0 array fails, the entire array fails.



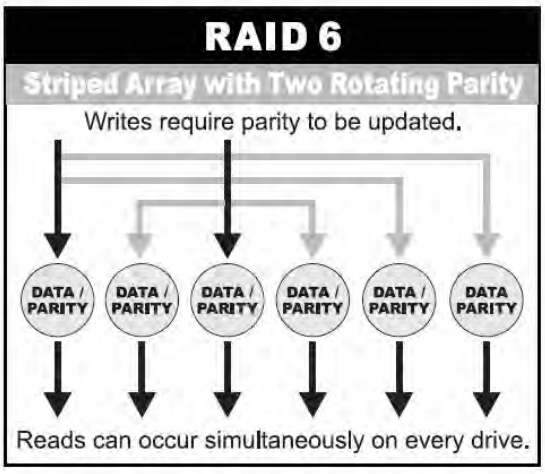
RAID 1, also known as disk mirroring, is simply a pair of disk drives that store duplicate data but appear to the computer as a single drive. Although striping is not used within a single mirrored drive pair, multiple RAID 1 arrays can be striped together to create a single large array consisting of pairs of mirrored drives. All writes must go to both drives of a mirrored pair so that the information on the drives is kept identical. However, each individual drive can perform simultaneous, independent read operations. Mirroring thus doubles the read performance of a single non-mirrored drive and while the write performance is unchanged. RAID 1 delivers the best performance of any redundant array type. In addition, there is less performance degradation during drive failure than in RAID 5 arrays.



Under **RAID 5** parity information is distributed across all the drives. Since there is no dedicated parity drive, all drives contain data and read operations can be overlapped on every drive in the array. Write operations will typically access one data drive and one parity drive. However, because different records store their parity on different drives, write operations can usually be overlapped.



RAID 6 is similar to RAID 5 in that data protection is achieved by writing parity information to the physical drives in the array. With RAID 6, however, ***two*** sets of parity data are used. These two sets are different, and each set occupies a capacity equivalent to that of one of the constituent drives. The main advantage of RAID 6 is High data availability – any two drives can fail without loss of critical data.



Dual-level RAID achieves a balance between the increased data availability inherent in RAID 1 and RAID 5 and the increased read performance inherent in disk striping (RAID 0). These arrays are sometimes referred to as RAID 0+1 or RAID 10 and RAID 0+5 or RAID 50.

In summary:

- RAID 0 is the fastest and most efficient array type but offers no fault-tolerance. RAID 0 requires a minimum of one drive.
- RAID 1 is the best choice for performance-critical, fault-tolerant environments. RAID 1 is the only choice for fault-tolerance if no more than two drives are used.
- RAID 5 combines efficient, fault-tolerant data storage with good performance characteristics. However, write performance and performance during drive failure is slower than with RAID 1. Rebuild operations also require more time than with RAID 1 because parity information is also reconstructed. At least three drives are required for RAID 5 arrays.
- RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two-dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures. It is a perfect solution for mission critical applications.

1.4 Array Definition

1.4.1 Drive Group

A Drive Group is a group of physical drives attached to the RAID controller, and where one or more Virtual Drives (VD) can be created. All Virtual Drives in the Drive Group use all of the physical drives in the Drive Group.

It is not possible to have multiple Disk Groups on the same physical disks. If physical disks of different capacity are grouped together in a Drive Group, then the capacity of the smallest disk will become the effective capacity of all the disks in the Drive Group.

1.4.2 Virtual Drive

A Virtual Drive is seen by the operating system as a single drive or logical device. A Virtual Drive is a storage unit created by the RAID controller from one or more physical drives. If there is an existing Drive Group and there is available Free Space, then a new Virtual Drive can still be created.

Depending on the RAID level used, the Virtual Drive may retain redundant data in case of a drive failure.

Chapter 2 Getting Started

2.1 Packaging, Shipment and Delivery

- Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- Unpack the subsystem and verify that the contents of the shipping carton are all there and in good condition.
- Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

2.2 Unpacking the NAS System

The package contains the following items:

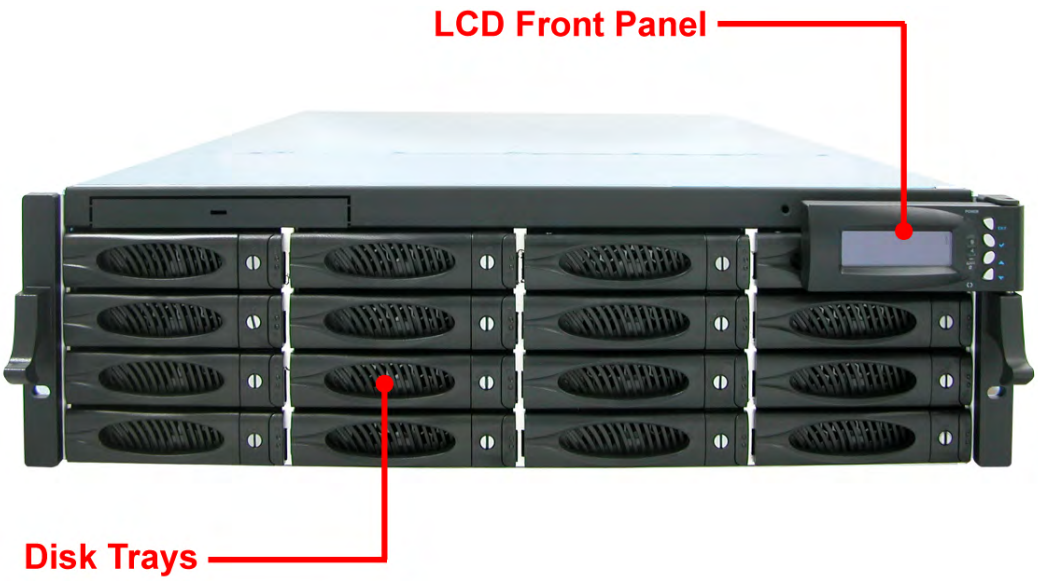
NAS System Unit	
Two (2) power cords	
Three (3) Ethernet LAN cables	
One (1) external serial cable	
One (1) RS232 null modem cable (phone jack to DB9)	
One (1) USB-to-PS/2 converter cable	
Installation Reference Guide	
Spare screws, etc.	

If any of these items are missing or damaged, please contact your dealer or sales representative for assistance.

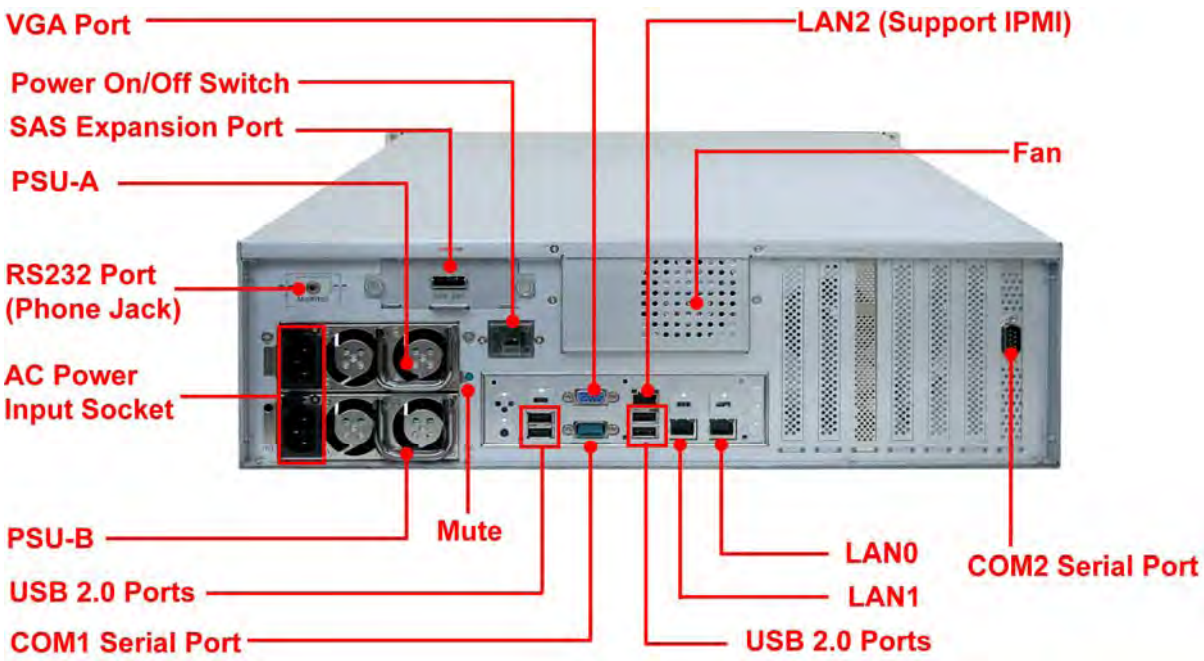
2.3 Identifying Parts of the NAS System

The illustrations below identify the various parts of the subsystem.

2.3.1 Front View



2.3.2 Rear View



1. **Mute** – Use the mute button to stop the power supply buzzer alarm.
2. **LAN Ports** – The system comes with three 1Gigabit Ethernet ports LAN0 (eth0) LAN1 (eth1) and LAN2 (eth2).
3. **SAS Expansion Port** – For connecting to SAS Expansion Chassis.
4. **COM1 and COM2 Serial Ports** – The system has two serial ports COM1 and COM2.
5. **Power On/Off Switch** – Use this switch to power on the system.
6. **Power Supply A, B** – Two power supplies PSU-A and PSU-B are located at the rear of the NAS system.
7. **AC Power Input Socket** – Use this to plug in the power cable connected from power source.
8. **USB 2.0 ports** – Four USB ports are located at the rear of the system.

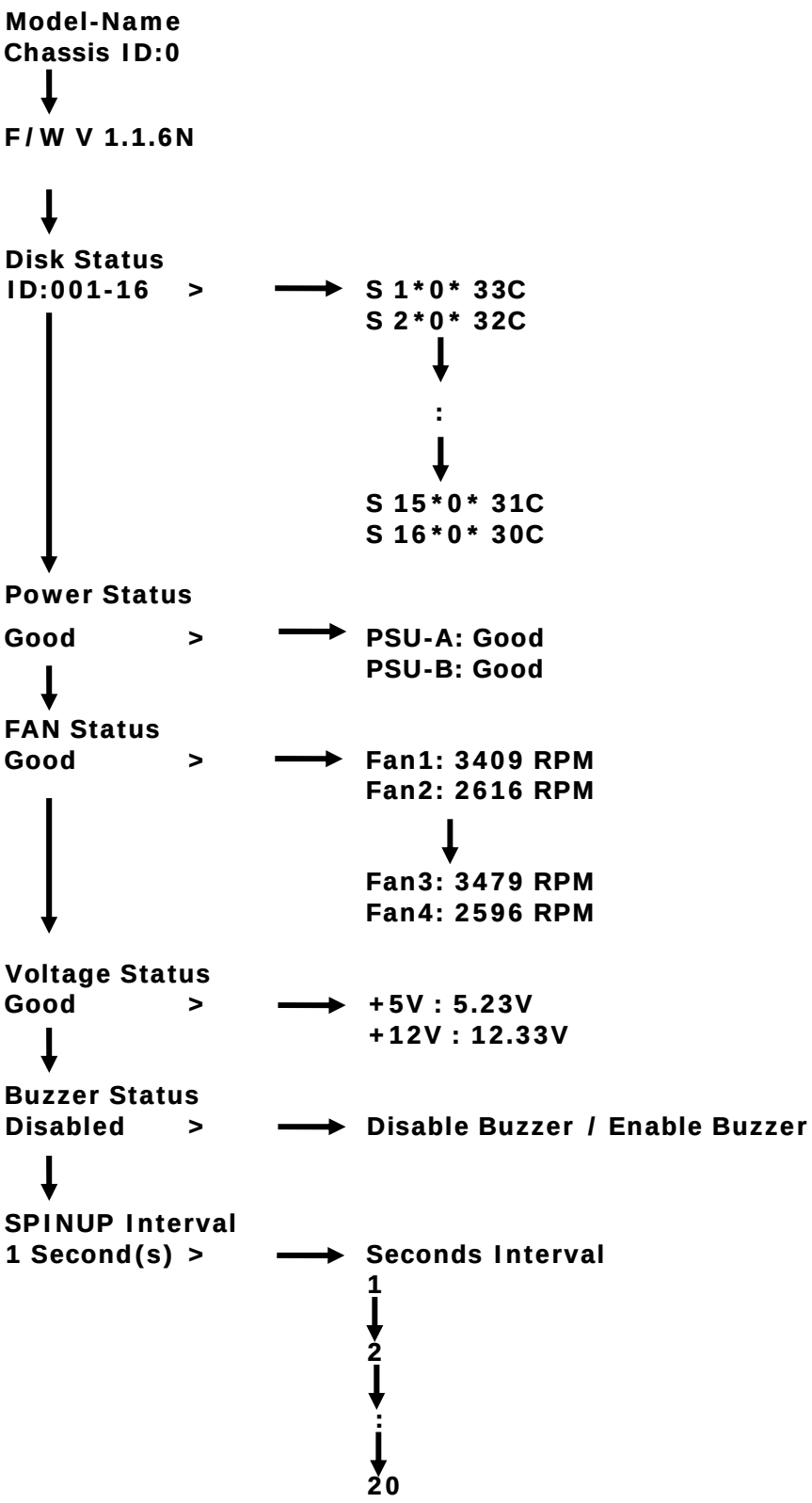
2.3.3 LCD Display Panel

2.3.3.2 LCD Front Panel Function Keys

PARTS	FUNCTION
Up and Down Arrow buttons ▲▼	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu.
Select button ✔	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu.

Use the function keys to navigate through the menus in the front panel. The menus will show the JBOD SAS Expander Board firmware version, disk status, fan status, voltage status, and allows you to disable or enable the alarm buzzer.

Menu Diagram



2.4 Drive Carrier Module

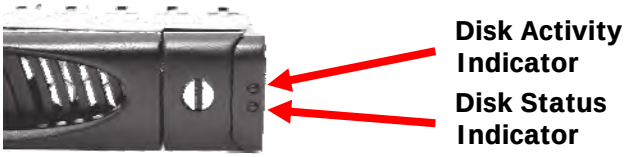
The Drive Carrier Module houses a 3.5 inch hard disk drive. It is designed for maximum airflow and incorporates a carrier locking mechanism to prevent unauthorized access to the HDD.

2.4.1 Disk Drive Status Indicators

Every Drive Carrier has 2 status indicator lights. One indicator light is used for Power On/Error. When this light is **GREEN** the power is on and everything is functioning normally. When the Power On/Error light is **RED**, then an error has occur that requires the user's attention.

The other status indicator light is the hard disk drive access light. When the hard disk drive is being accessed, this light will flash **BLUE**.

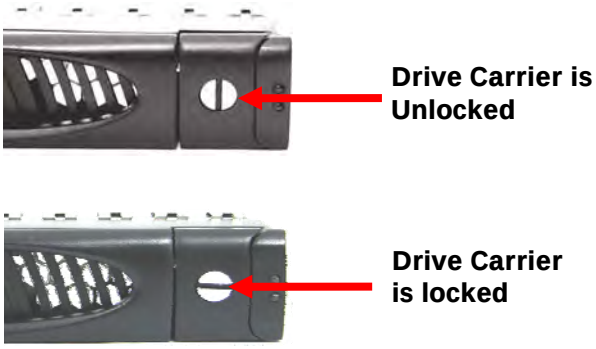
In addition, both indicator lights are viewable within a 170° arc.



2.4.2 Lock Indicator

Every Drive Carrier is lockable and is fitted with a lock indicator to indicate whether or not the carrier is locked into the chassis or not. Each carrier is also fitted with an ergonomic handle for easy carrier removal.

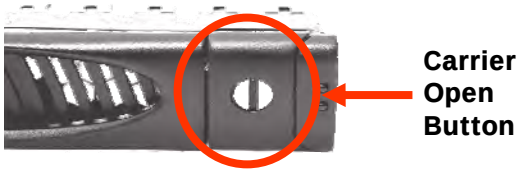
When the Lock Groove is horizontal, this indicates that the Drive Carrier is locked. When the Lock Groove is vertical, then the Drive Carrier is unlocked. Lock and unlock the Drive Carriers by using a flat-head screw driver.



2.5 Installing Hard Drives

This section describes the physical locations of the hard drives supported by the NAS system and give instructions on installing a hard drive. The system supports hot-swapping allowing you to install or replace a hard drive while the NAS system is running.

a. To remove a drive tray, make sure it is in unlocked position. Then press the carrier open button. The Drive Carrier handle will flip open.



c. Pull out an empty disk tray. Pull the handle outwards to remove the carrier from the enclosure.

d. Place the hard drive in the disk tray. Make sure the holes of the disk tray align with the holes of the hard drive.

e. Install the mounting screws on the bottom part to secure the drive in the disk tray.

f. Slide the tray into a slot.

g. Close the handle until you hear the latch click into place.

2.6 Preparing the System

1. Attach network cable to Ethernet port LAN0. Connect the other end to your network switch. You may also connect the other Ethernet LAN1 port if needed.
2. Connect monitor to the VGA port.
3. Connect PS/2 keyboard and mouse to the USB-to-PS/2 converter cable, and then connect the USB connector to the USB port on the NAS.

2.7 Powering On

1. Plug in the two power cords into the AC Power Input Socket of PSU located at the rear of the NAS system.

NOTE: The NAS system is equipped with redundant, full range power supplies with PFC (power factor correction). The system will automatically select voltage.

2. Open the protective cover of the Power On/Off Switch.
3. Press the Power On/Off Switch to power on the NAS.
4. The Power LED on the front Panel will turn green.
5. Follow the steps in the next chapter to configure a RAID.
6. Follow the steps in the succeeding chapters to configure the NAS system.

Chapter 3 RAID Configuration and Management

Before using the NAS system, a RAID configuration must be created. At least one virtual drive is required to be used in the NAS. You may create more than one Virtual Drive if needed.

3.1 WebBIOS Configuration Utility

The WebBIOS Configuration Utility (CU) enables you to create and manage RAID configurations on LSI SAS controllers. The WebBIOS CU resides in the SAS controller BIOS and operates independently of the operating system.

NOTE: For additional information about the LSI MegaRAID SAS RAID Configuration and Management, please visit LSI web site: http://www.lsi.com/DistributionSystem/AssetDocument/files/docs/techdocs/storage_stand_prod/sas/mr_sas_sw_ug.pdf

3.1.1 Starting the WebBIOS Configuration Utility

Perform the following steps to enter the WebBIOS Configuration Utility when you boot the system.

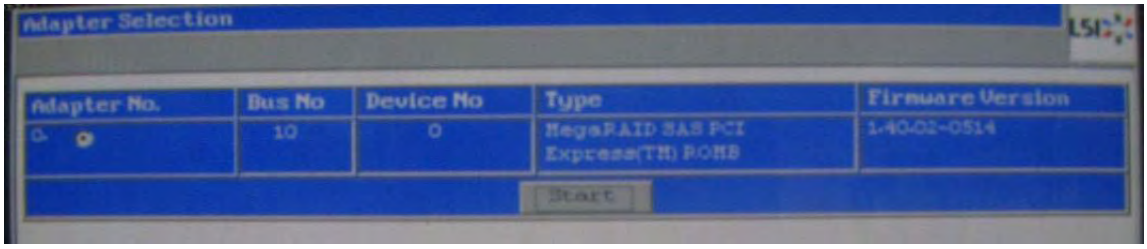
1. When the host computer is booting, hold down the <Ctrl> key and press the <H> key when the following text appears on the screen:

   LSI MegaRAID SAS-MFI BIOS
   Version x.xx.xx
   Copyright© LSI Corporation

   Press <Ctrl><H> for WebBIOS CU

   The Adapter Selection screen appears.

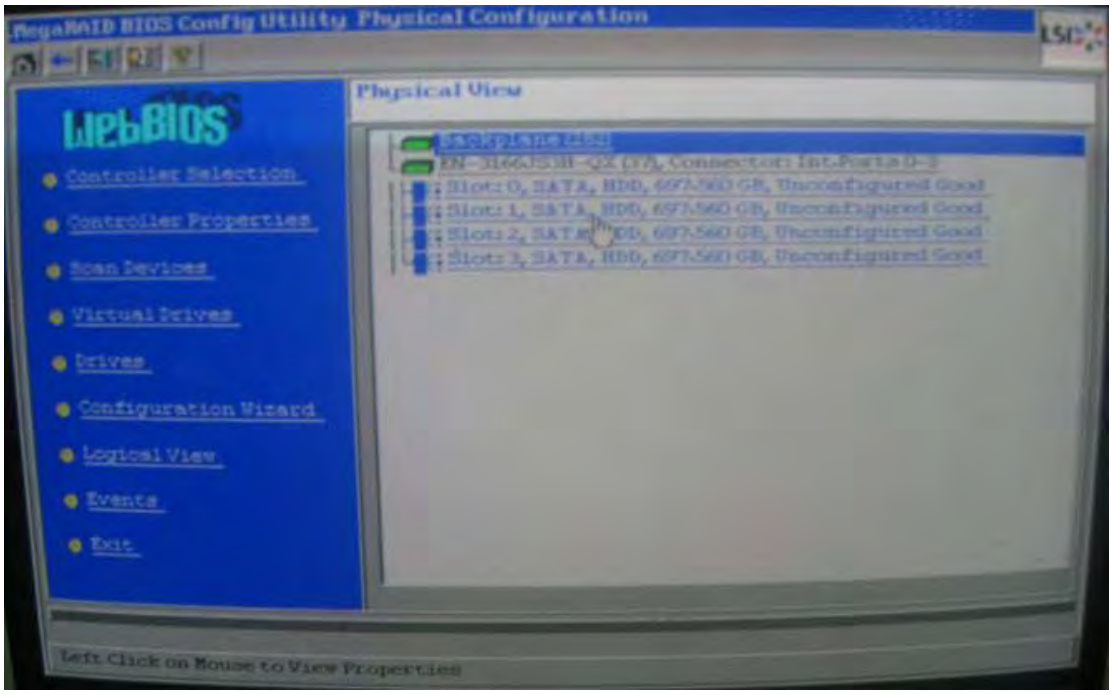
2. Select the SAS MegaRAID Adapter, if not selected.



4. Click **Start** to continue. The main WebBIOS CU screen appears.

3.1.2 WebBIOS CU Main Screen Options

The figure below shows the screen when you start the WebBIOS CU and select an adapter.



In the lower right panel, the logical view part of the screen displays all of the virtual drives that are configured on this controller. In the upper right panel, the physical view part of the screen displays the drives that are connected to the controller.

To toggle between the physical view and logical view of the storage devices connected to the controller, click **Physical View** or **Logical View** in the menu on the left. When the physical view screen is displayed, the lower right panel displays the drive groups that are configured on this controller.

For drives in an enclosure, the screen displays the drive information in the following format: (Connector): position: slot. The connector information identifies where the chain of enclosures is connected to the RAID controller. The position number identifies the position of the enclosure in the daisy chain.

Directly-attached drives displays in the following format: Slot.

The toolbar at the top of the WebBIOS CU has the following buttons:

Table 3.1.2 WebBIOS CU Toolbar Icons

Icon	Description
	Click this icon to return to the main screen from any other WebBIOS CU screen.
	Click this icon to return to the previous screen that you were viewing.
	Click this icon to exit the WebBIOS CU program.
	Click this icon to display the Adapter Selection screen. If the computer system has multiple controllers, you use this screen to view the devices connected to a different controller.
	Click this icon to turn off the sound on the onboard controller alarm.
	Click this icon to display information about the WebBIOS CU version, browser version, and HTML interface engine.

The WebBIOS CU Main Screen contains the following options:

- **Controller Selection:** Select this to view the Adapter Selection screen, where you can select a different SAS controller. You can then view information about the controller and the devices connected to it, or create a new configuration on the controller.
- **Controller Properties:** Select this to view the properties of the currently selected SAS controller.
- **Scan Devices:** Select this to have the WebBIOS CU re-scan the physical and virtual drives for any changes in the drive status or the physical configuration. The WebBIOS CU displays the results of the scan in the physical and virtual drive descriptions.
- **Virtual Drives:** Select this to view the Virtual Disks screen, where you can change and view virtual drive properties, delete virtual drives, initialize drives, and perform other tasks.
- **Drives:** Select this to view the Drives screen, where you can view drive properties, create hot spares, and perform other tasks.
- **Configuration Wizard:** Select this to start the Configuration Wizard and create a new storage configuration, clear a configuration, or add a configuration.
- **Physical View/Logical View:** Select this to toggle between the Physical View and Logical View screens.
- **Events:** Select this to view system events in the Event Information screen.
- **Exit:** Select this to exit the WebBIOS CU and continue with system boot

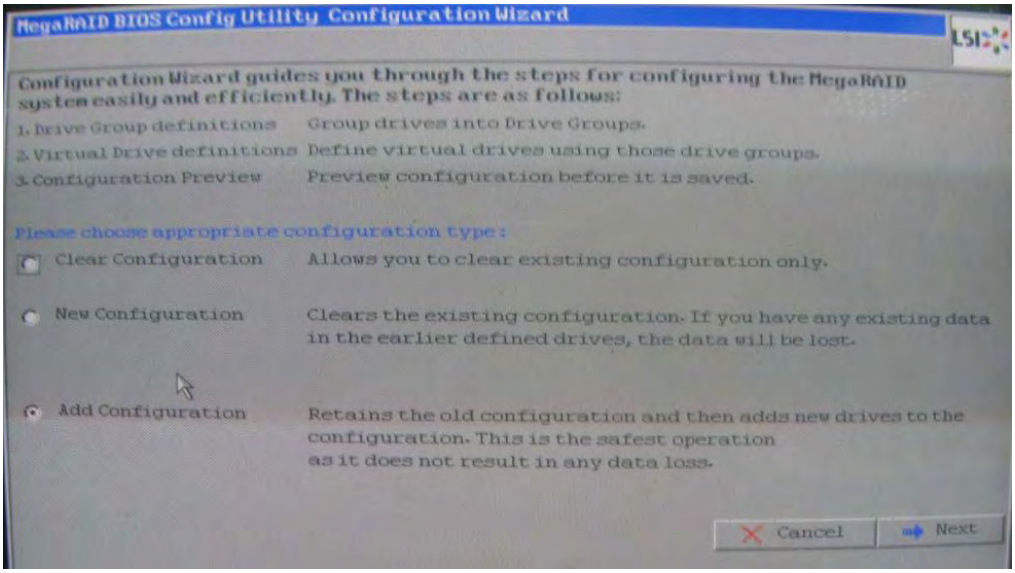
3.2 Configuring RAID Drive Groups and Virtual Drives

NOTE: This section describes the steps to create two RAID Level 5 Virtual Drives to be used in the NAS system.

For additional information about the LSI MegaRAID SAS RAID Configuration and Management, please visit the LSI web site: http://www.lsi.com/DistributionSystem/AssetDocument/files/docs/techdocs/storage_stand_prod/sas/mr_sas_sw_ug.pdf

To create a RAID configuration:

1. Click **Configuration Wizard** on the WebBIOS main screen. The first Configuration Wizard screen is displayed.


MegaRAID BIOS Config Utility Configuration Wizard
LSI
Configuration Wizard guides you through the steps for configuring the MegaRAID system easily and efficiently. The steps are as follows:
1. Drive Group definitions
Group drives into Drive Groups.
2. Virtual Drive definitions
Define virtual drives using those drive groups.
3. Configuration Preview
Preview configuration before it is saved.
Please choose appropriate configuration type:
Clear Configuration
Allows you to clear existing configuration only.
New Configuration
Clears the existing configuration. If you have any existing data in the earlier defined drives, the data will be lost.
Add Configuration
Retains the old configuration and then adds new drives to the configuration. This is the safest operation as it does not result in any data loss.
Cancel
Next

2. Select a configuration option.

WARNING: If you choose the first or second option, all existing data in the configuration will be deleted. Make a backup of any data that you want to keep before you choose an option.

- **Clear Configuration:** Clears the existing configuration.
- **New Configuration:** Clears the existing configuration and lets you create a new configuration.
- **Add Configuration:** Retains the existing storage configuration and adds new drives to it (this does not cause any data loss).

3. To create a new configuration, select **New Configuration**. Click **Next**.

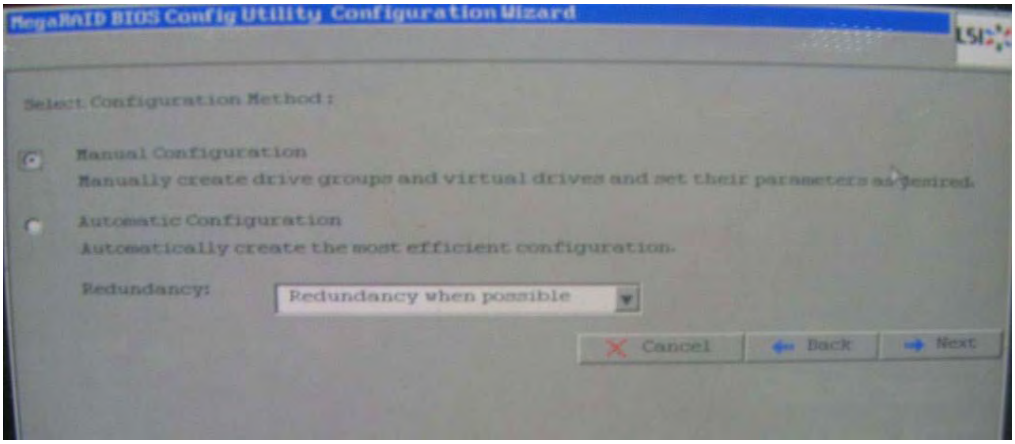
   A dialog box will warn that you will lose data if you select Clear Configuration or New Configuration.

NOTE: You only select New Configuration the first time you create the drive group and virtual drives. When you add more drives and create new drive groups or virtual drives, you need to select Add Configuration.

4. On the next screen, select **Manual Configuration**.

   Types of Configuration Methods:

   - **Manual Configuration:** Allows you to control all attributes of the new storage configuration.
   - **Automatic Configuration with Redundancy:** Automatically creates an optimal RAID 1, RAID 5, or RAID 6 configuration, providing data redundancy.
   - **Automatic Configuration without Redundancy:** Automatically creates a non-redundant RAID 0 configuration.



5. Click **Next** to continue.

3.2.1 Using Auto Configuration

If you select one of the Auto Configuration options, either with or without redundancy, the following are the steps to configure RAID:

1. When WebBIOS displays the proposed new configuration, review the information on the screen, and click **Accept** to accept it. (Or click **Back** to go back and change the configuration.)

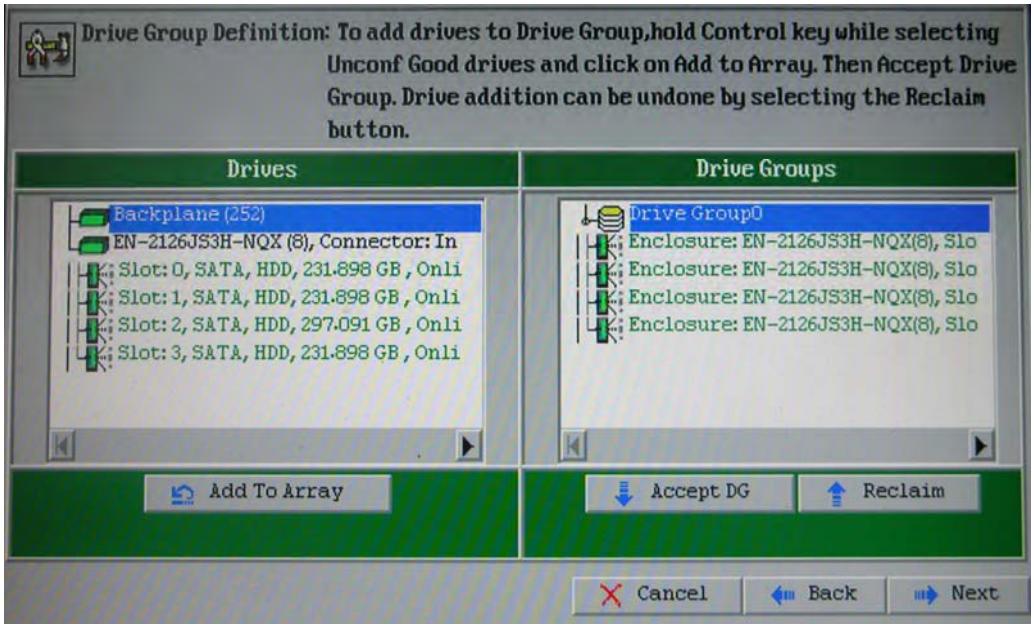
    - **RAID 0:** If you select **Automatic Configuration without Redundancy**, WebBIOS creates a RAID 0 configuration.
    - **RAID 1**: If you select **Automatic Configuration with Redundancy**, and only two drives are available, WebBIOS creates a RAID 1 configuration.
    - **RAID 5**: If you select **Automatic Configuration with Redundancy**, and three or more drives are available, WebBIOS creates a RAID 5 configuration.
    - **RAID 6**: If you select **Automatic Configuration with Redundancy**, and the RAID 6 option is enabled, and three or more drives are available, WebBIOS creates a RAID 6 configuration.
2. Click **Yes** when you are prompted to save the configuration.
3. Click **Yes** when you are prompted to initialize the new virtual drive(s). WebBIOS CU begins a background initialization of the virtual drives.

3.2.2 Using Manual Configuration: Creating RAID 5 Virtual Drives

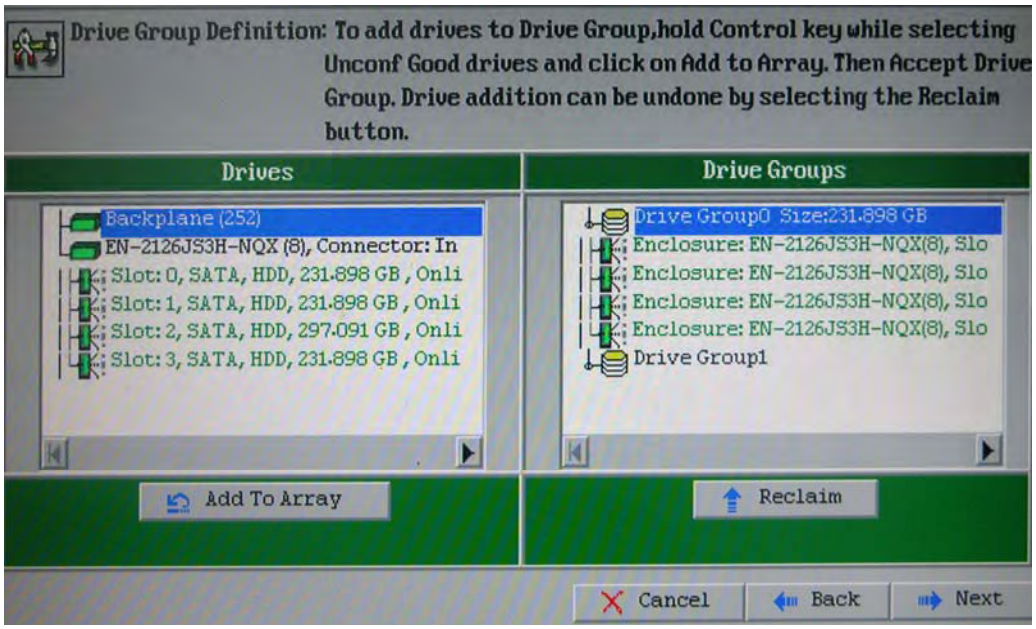
When you select **Custom Configuration** and click **Next**, the Drive Group Definition screen appears. You use this screen to select drives to create drive groups.

1. Hold <Ctrl> while you select at least three ready drives in the Physical Drives panel on the left.
2. Click **Add to Array** to move the drives to a proposed drive group configuration in the Drive Groups panel on the right.

   If you need to undo the changes, click the **Reclaim** button.

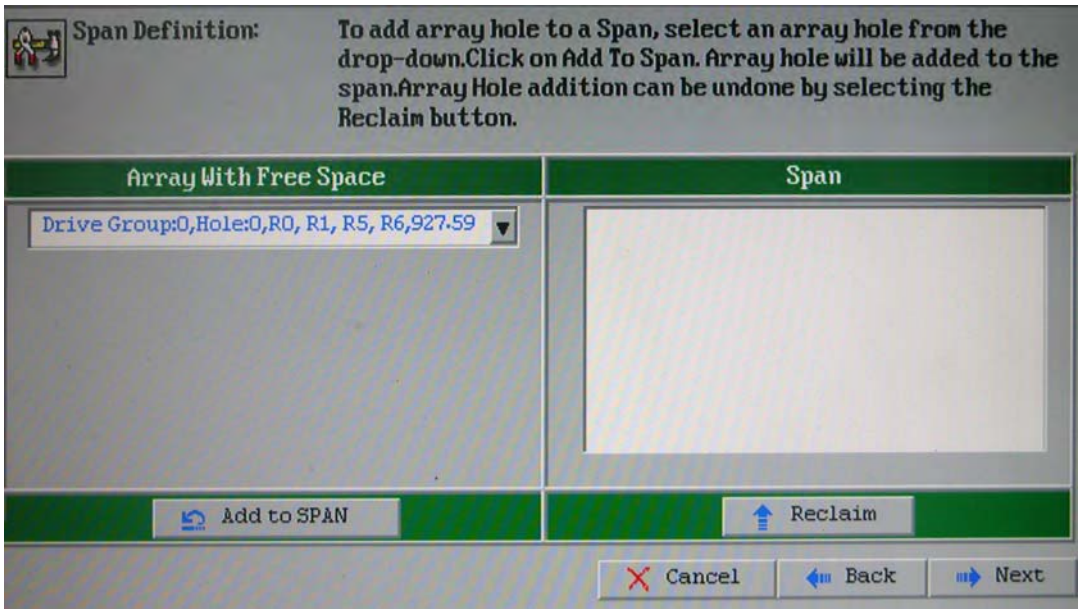

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.
Drives
Drive Groups
Backplane (252)
EN-2126JS3H-NQX (8), Connector: In
Slot: 0, SATA, HDD, 231.898 GB , Onli
Slot: 1, SATA, HDD, 231.898 GB , Onli
Slot: 2, SATA, HDD, 297.091 GB , Onli
Slot: 3, SATA, HDD, 231.898 GB , Onli
Drive Group0
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Add To Array
Accept DG
Reclaim
Cancel
Back
Next

3. When you have finished selecting drives for the drive group, click **Accept DG.**

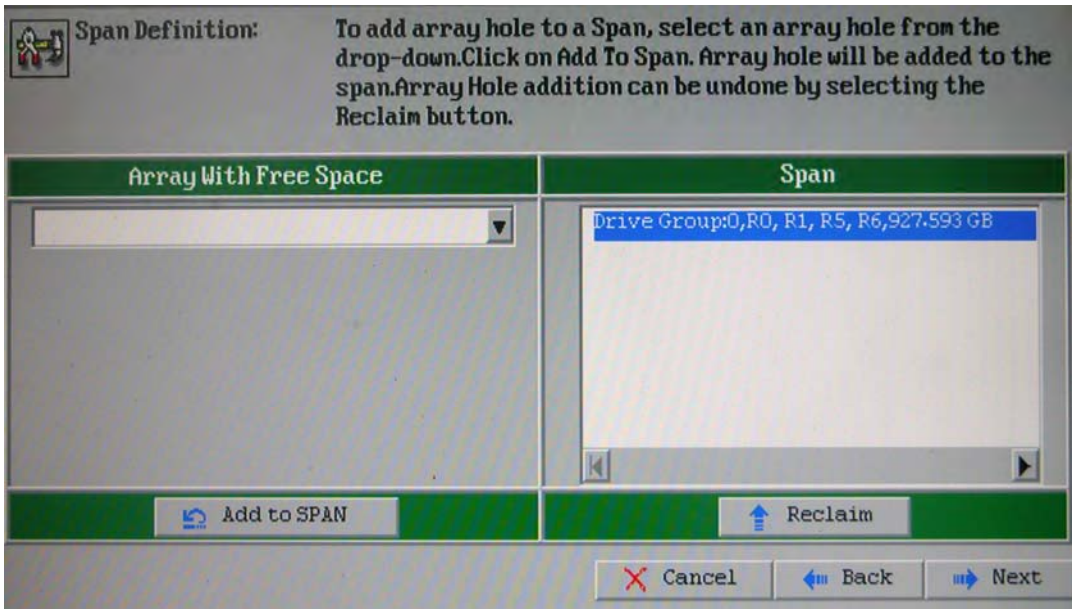

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.
Drives
Drive Groups
Backplane (252)
EN-2126JS3H-NQX (8), Connector: In
Slot: 0, SATA, HDD, 231.898 GB , Onli
Slot: 1, SATA, HDD, 231.898 GB , Onli
Slot: 2, SATA, HDD, 297.091 GB , Onli
Slot: 3, SATA, HDD, 231.898 GB , Onli
Drive Group0 Size:231.898 GB
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Enclosure: EN-2126JS3H-NQX(8), Slo
Drive Group1
Add To Array
Reclaim
Cancel
Back
Next

4. Click **Next**.

5. The Span Definition screen appears. Drive Group 0 is shown in the Array With Free Space list. Click **Add to SPAN**.


Span Definition:
To add array hole to a Span, select an array hole from the drop-down.Click on Add To Span. Array hole will be added to the span.Array Hole addition can be undone by selecting the Reclaim button.
Array With Free Space
Span
Drive Group:0,Hole:0,R0, R1, R5, R6,927.59
Add to SPAN
Reclaim
Cancel
Back
Next

6. Drive Group 0 is listed in the Span panel. Click **Next**.


Span Definition:
To add array hole to a Span, select an array hole from the drop-down.Click on Add To Span. Array hole will be added to the span.Array Hole addition can be undone by selecting the Reclaim button.
Array With Free Space
Span
Drive Group:0,R0, R1, R5, R6,927.593 GB
Add to SPAN
Reclaim
Cancel
Back
Next

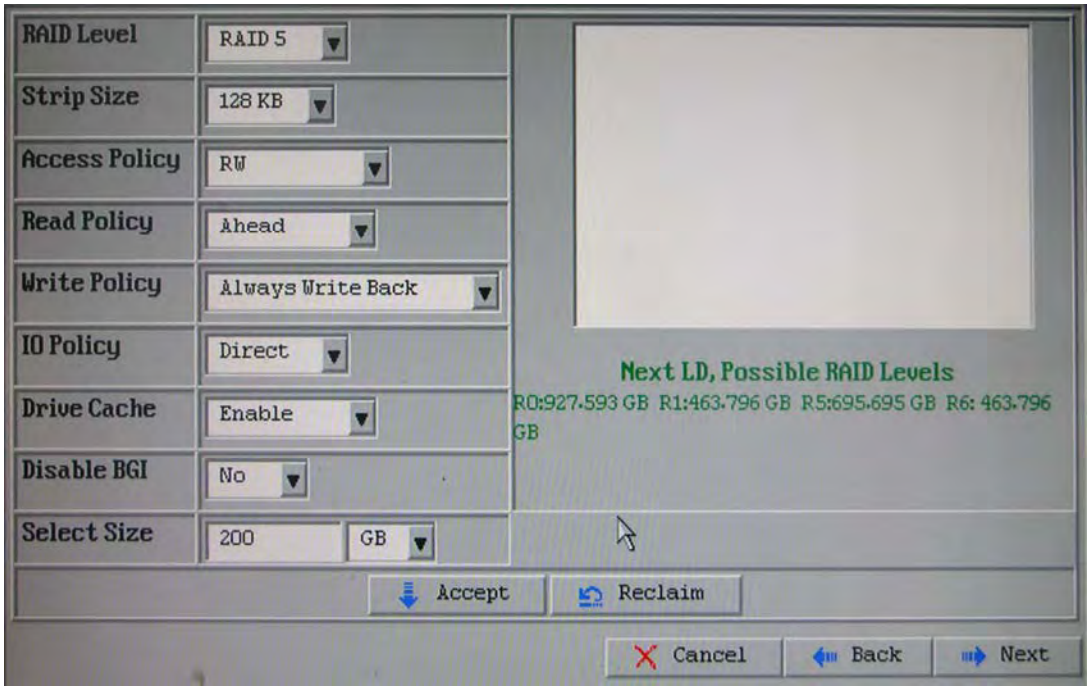
7. The Virtual Drive Definition screen appears. You use this screen to select the RAID level, stripe size, read policy and other attributes for the new virtual drives.

Virtual Drive Parameters and Descriptions

Parameter	Description
RAID Level	The drop-down menu lists the possible RAID levels for the virtual drive.
Stripe Size	The stripe size specifies the length of the data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider a stripe that contains 64 KB of drive space and has 16 KB of data residing on each drive in the stripe. In this case, the stripe size is 64 KB and the strip size is 16 KB. You can set the stripe size to 8, 16, 32, 64, 128, 256, 512, and 1024 Kbytes. A larger stripe size produces higher read performance. If your computer regularly performs random read requests, choose a smaller stripe size. The default is 64 Kbytes.
Access Policy	Select the type of data access that is allowed for this virtual drive: ➢ *RW*: Allow read/write access. This is the default. ➢ *Read Only*: Allow read-only access. ➢ *Blocked*: Do not allow access.
Read Policy	Specify the read policy for this virtual drive: ➢ *Normal*: This disables the read ahead capability. This is the default. ➢ *Ahead*: This enables read ahead capability, which allows the controller to read sequentially ahead of requested data and to store the additional data in cache memory, anticipating that the data will be needed soon. This speeds up reads for sequential data, but there is little improvement when accessing random data. ➢ *Adaptive*: When Adaptive read ahead is selected, the controller begins using read ahead if the two most recent drive accesses occurred in sequential sectors. If the read requests are random, the controller reverts to *Normal* (no read ahead).

Write Policy	Specify the write policy for this virtual drive: ➢ *Always Write Back*: In Writeback mode the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. This setting is recommended in Standard mode. ➢ *Write Through*: In Writethrough mode the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction. This is the default. ➢ *Write Back with BBU*: Select this mode if you want the controller to use Writeback mode but the controller has no BBU or the BBU is bad. If you do not choose this option, the controller firmware automatically switches to Writethrough mode if it detects a bad or missing BBU. Caution: LSI allows Writeback mode to be used with or without a battery. LSI recommends that you use **either** a battery to protect the controller cache, or an uninterruptible power supply (UPS) to protect the entire system. If you do not use a battery or a UPS, and there is a power failure, you risk losing the data in the controller cache.
IO Policy	The IO Policy applies to reads on a specific virtual drive. It does not affect the read ahead cache. ➢ *Direct*: In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to the cache and the host concurrently. If the same data block is read again, it comes from cache memory. This is the default. ➢ *Cached*: In Cached I/O mode, all reads are buffered in cache memory.
Drive Cache	Specify the drive cache policy: ➢ *Enable*: Enable the drive cache. ➢ *Disable*: Disable the drive cache. This is the default. ➢ *Unchanged*: Leave the current drive cache policy unchanged.
Disable BGI	Specify the background initialization status: ➢ *No*: Leave background initialization enabled. This means that a new configuration can be initialized in the background while you use WebBIOS to do other configuration tasks. This is the default. ➢ *Yes*: Select *Yes* if you do not want to allow background initializations for configurations on this controller.
Select Size	Specify the size of the virtual drive in megabytes. Normally, this would be the full size for RAID 5 shown in the Configuration panel on the right. You may specify a smaller size if you want to create other virtual drives on the same drive group.

To create Virtual Drive 0, select RAID 5 as RAID Level, and enter the size in Select Size. Click **Accept** then **Next**.

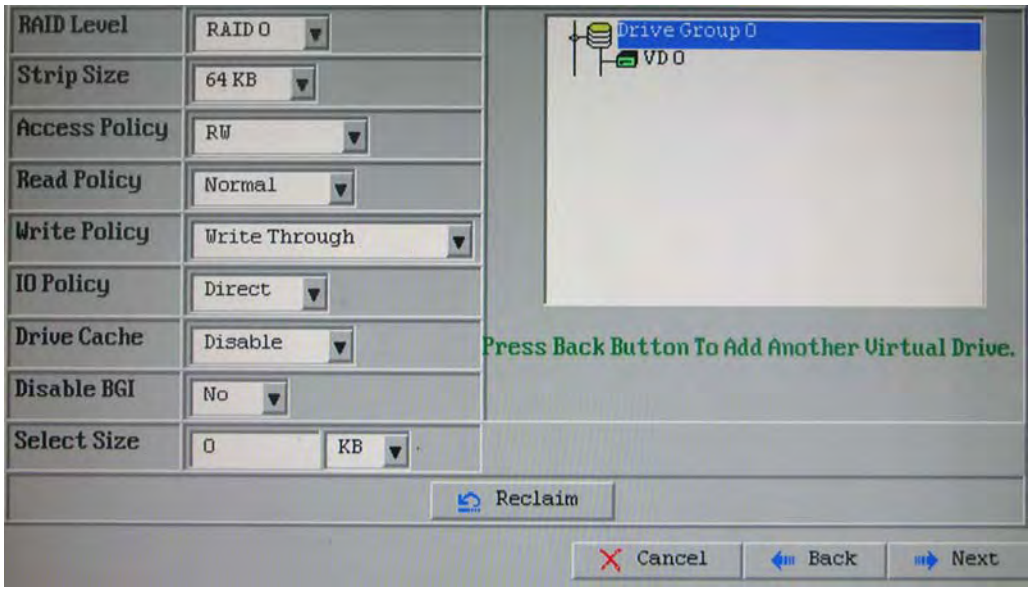


NOTE: The Virtual Drive can use all of the capacity of the Drive Group. You may create several Virtual Drives depending on your usage and requirement.

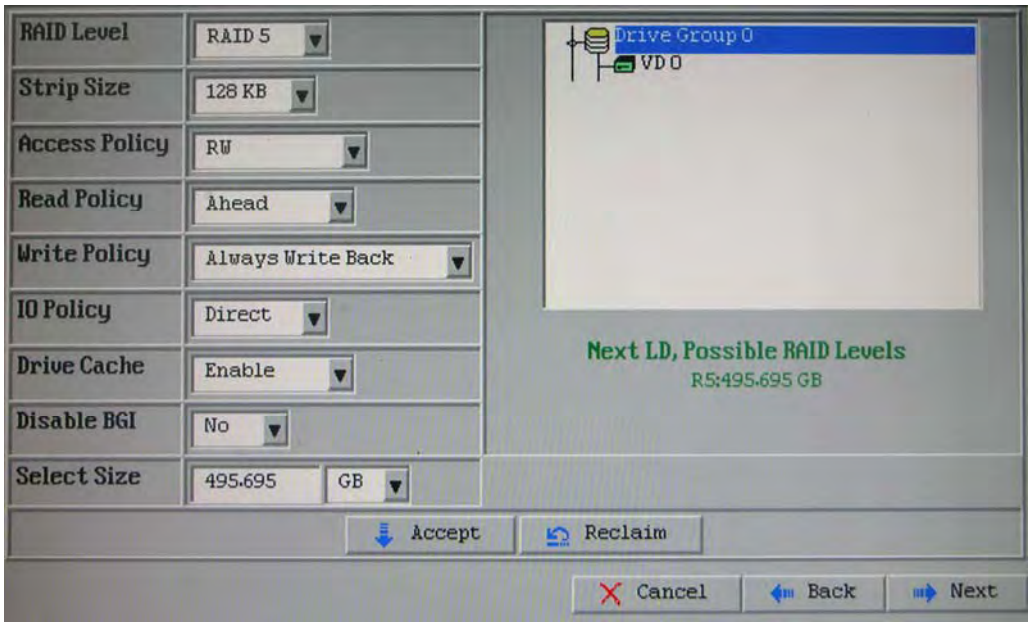
NOTE: For ProNAS 1.3.x version, the following RAID settings are recommended:

Stripe Size	**128 KB**
Read Policy	**Ahead**
Write Policy	**Always Write Back**
Drive Cache	**Enable**

8. VD 0 is created. To create the second Virtual Drive, click **Back**. The Span Definition will be displayed. Click **Add to SPAN** and **Yes**.



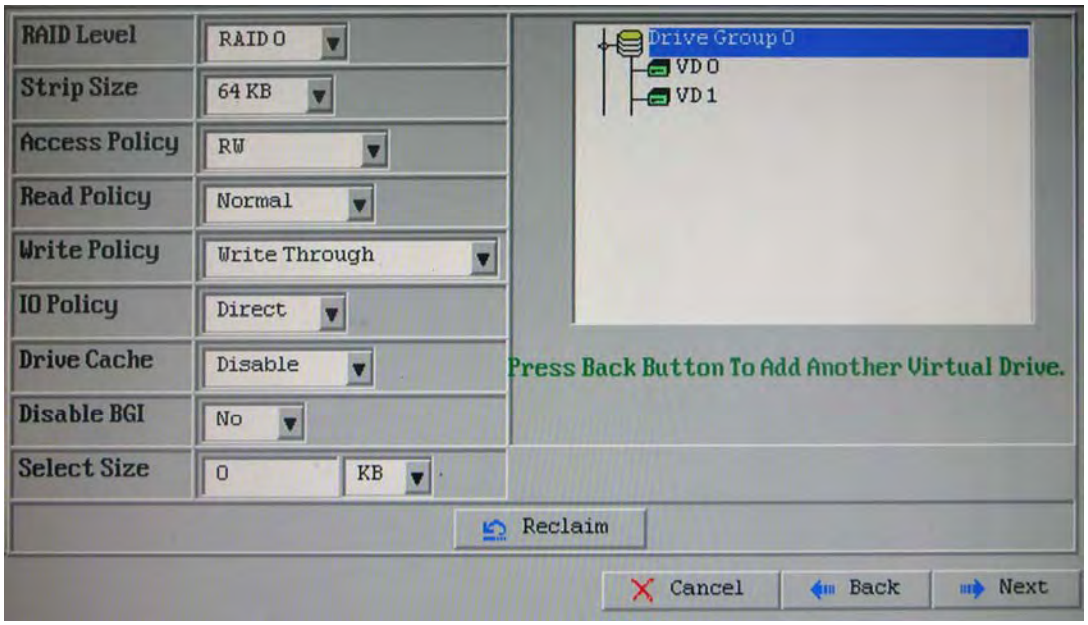
9. The Virtual Disk Definition screen appears. To create Virtual Drive 1, select RAID 5 as RAID Level. The remaining capacity of the Drive Group will be used by Virtual Drive 1. Select **Accept** and click **Next**.



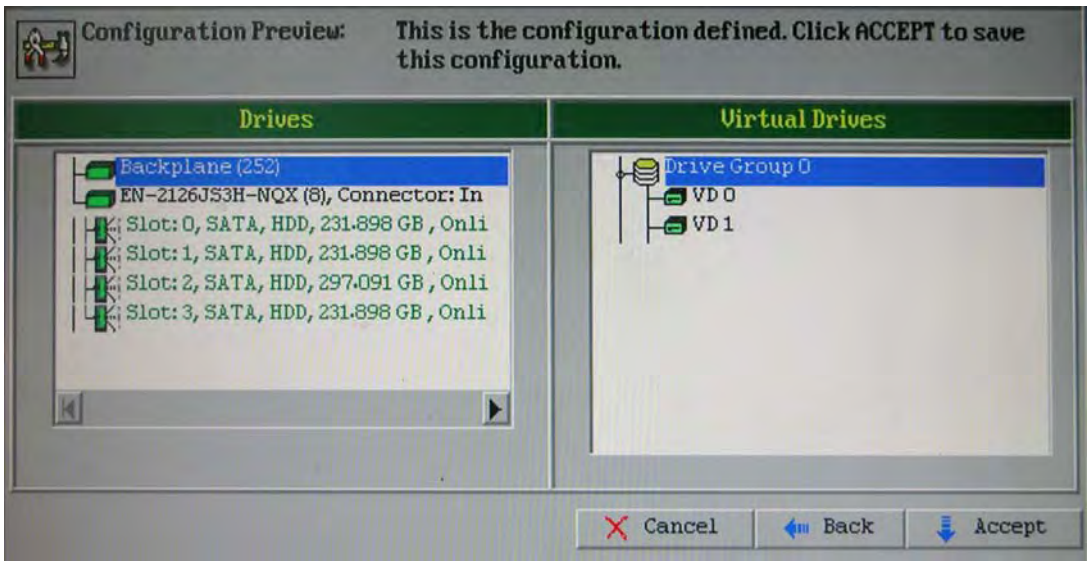
NOTE: For ProNAS 1.3.x version, the following RAID settings are recommended:

Stripe Size	**128 KB**
Read Policy	**Ahead**
Write Policy	**Always Write Back**
Drive Cache	**Enable**

10. Virtual Drive 1 is created. Click **Next**.

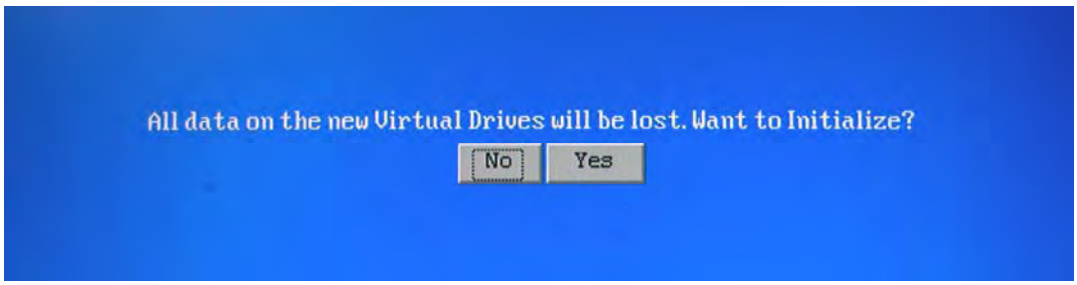


11. The Configuration Preview screen is shown. Click **Accept** to save the configuration.

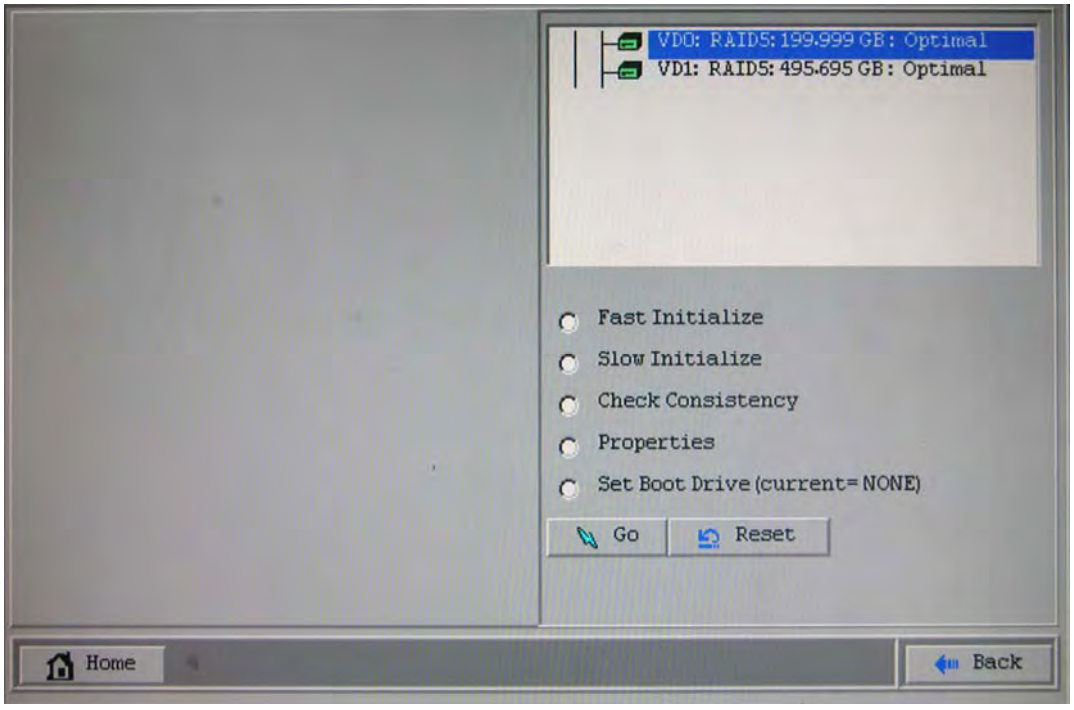

Configuration Preview:
This is the configuration defined. Click ACCEPT to save this configuration.
Drives
Virtual Drives
Backplane (252)
EN-2126JS3H-NQX (8), Connector: In
Slot: 0, SATA, HDD, 231.898 GB , Onli
Slot: 1, SATA, HDD, 231.898 GB , Onli
Slot: 2, SATA, HDD, 297.091 GB , Onli
Slot: 3, SATA, HDD, 231.898 GB , Onli
Drive Group 0
VD 0
VD 1
Cancel
Back
Accept

12. A Confirmation Page will be displayed. Select **Yes** to confirm.

13. Another Confirmation Page is displayed. Select **Yes** to initialize the Virtual Drives.



14. The two Virtual Drives will be initialized in the background. Click **Home** to return to the main screen of WebBIOS CU.

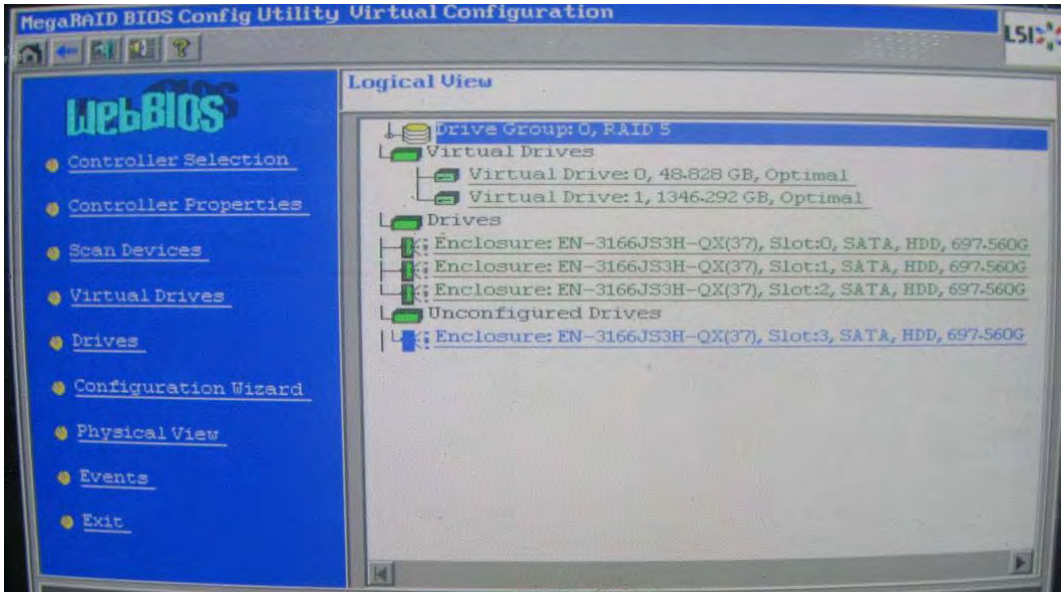


3.3 Creating Global Hot Spare

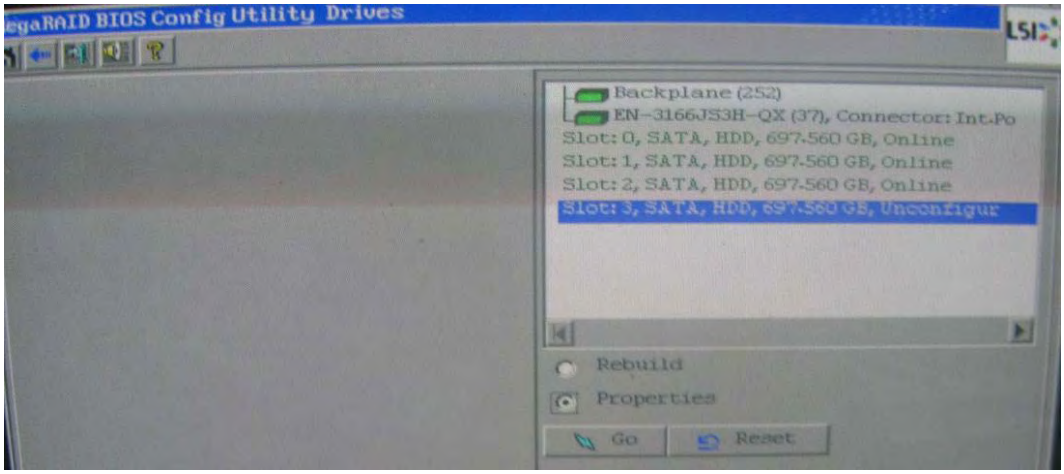
A global hot spare can be used to replace a failed physical disk in any redundant array as long as the capacity of the global hot spare is equal to or larger than the coerced capacity of the failed physical disk.

To create a global hot spare:

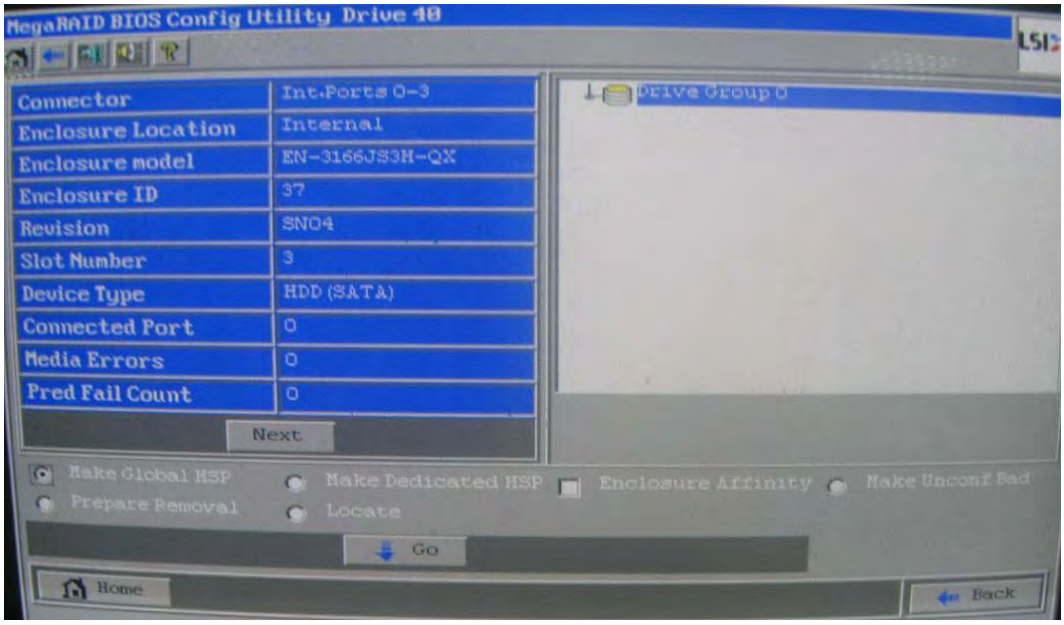
1. While in WebBIOS CU main screen, select **Drives** option.



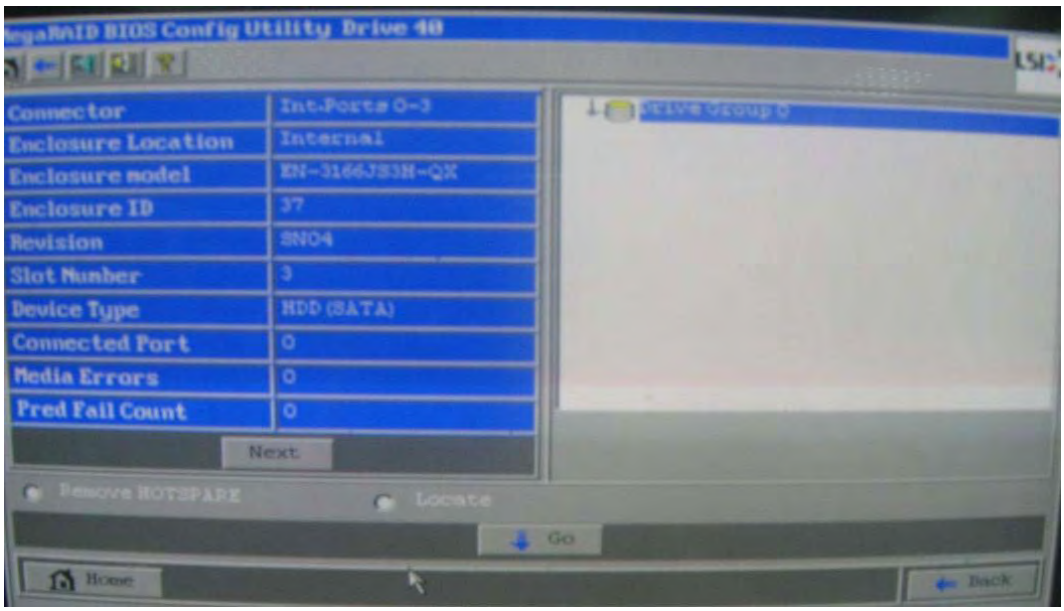
2. Select an un-configured drive and tick **Properties** the click **Go**.



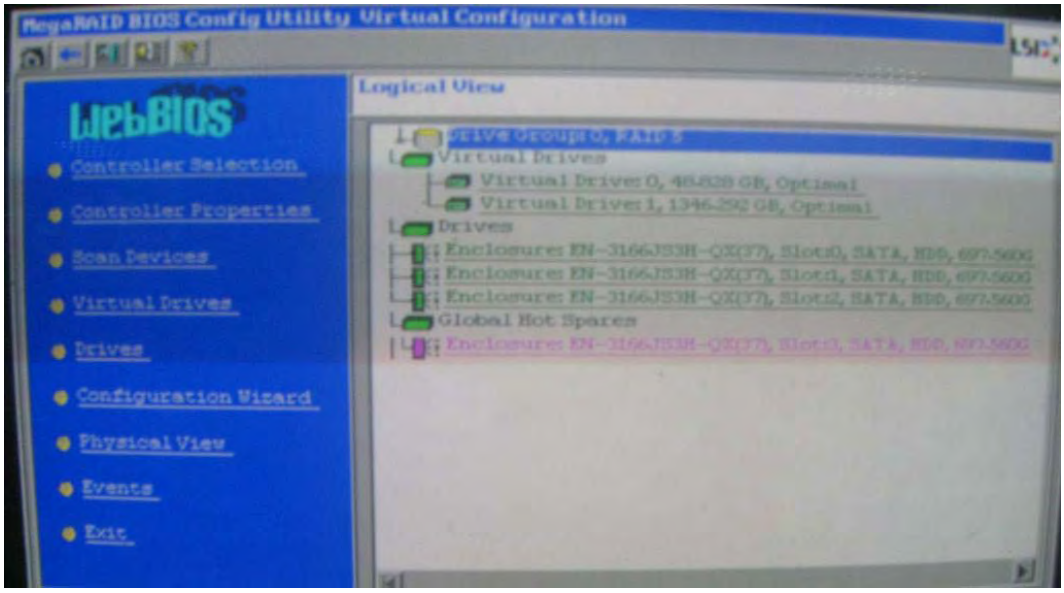
3. Choose the **Make Global HSP** option and click **Go**.



4. Click **Go**.

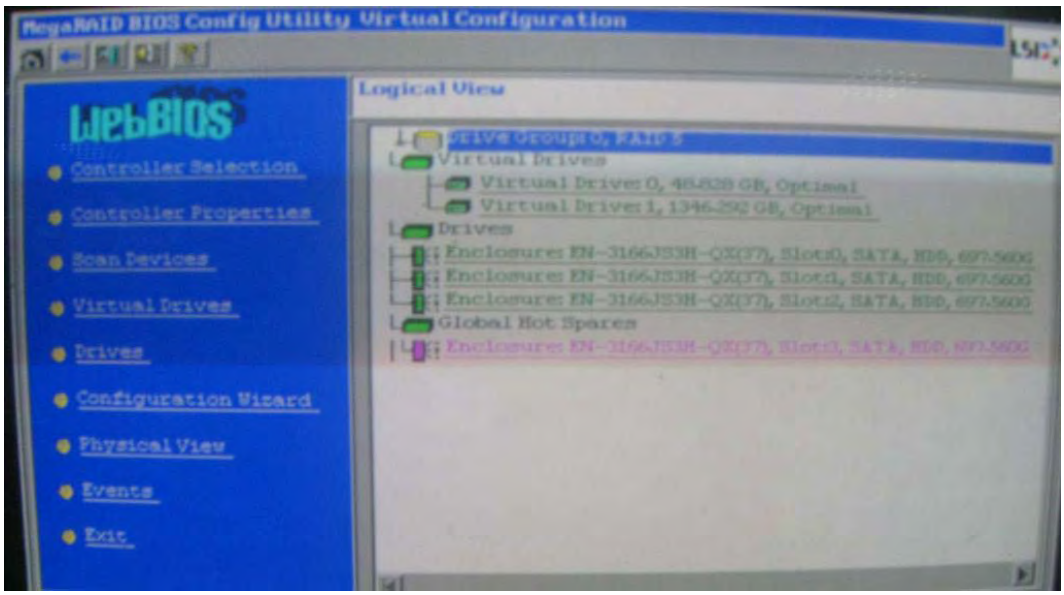


5. The global hot spare drive is created.



3.4 Restarting the Controller

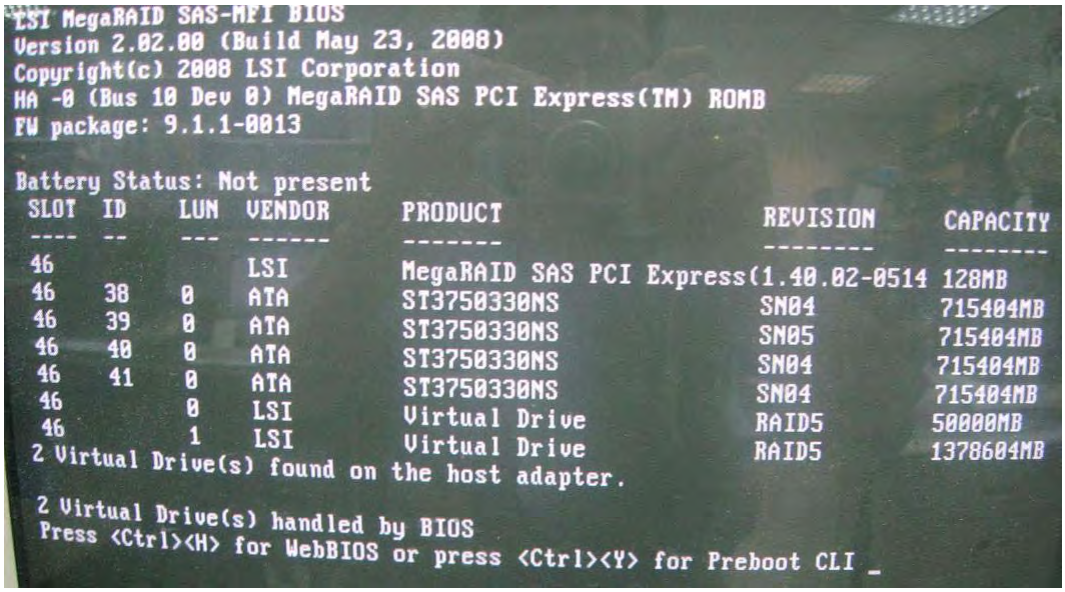
1. Verify the status of Virtual Drives.



2. Click **Exit**.
3. A confirmation screen will be displayed. Select **Yes**.

4. A message “Please Reboot your system.” Will be displayed. Reboot your system by pressing CTRL+ALT+DEL keys.

5. The system will reboot.


LSI MegaRAID SAS-MFI BIOS
Version 2.02.00 (Build May 23, 2008)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus 10 Dev 0) MegaRAID SAS PCI Express(TM) ROMB
FW package: 9.1.1-0013
Battery Status: Not present
SLOT ID LUN VENDOR PRODUCT REVISION CAPACITY
46 LSI MegaRAID SAS PCI Express(1.40.02-0514 128MB
46 38 0 ATA ST3750330NS SN04 715404MB
46 39 0 ATA ST3750330NS SN05 715404MB
46 40 0 ATA ST3750330NS SN04 715404MB
46 41 0 ATA ST3750330NS SN04 715404MB
46 0 LSI Virtual Drive RAID5 50000MB
46 1 LSI Virtual Drive RAID5 1378604MB
2 Virtual Drive(s) found on the host adapter.
2 Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS or press <Ctrl><Y> for Preboot CLI

6. The NAS system will be started. Please refer to Part 2 for the proNAS system configuration.

PART II proNAS System

Chapter 4 Introduction

The NAS system comes with “proNAS” NAS management solution and “proBackup” client backup solution as well as proNAS HA solution (optional) to provide the enterprises the most flexible, scalable, securable and manageable NAS environment. Administrator can centralize and easily manage the NAS nodes via Internet/Intranet and enhance greater data availability via proNAS.

4.1 proNAS Key Components

- **proNAS Manager**: Provides several management tools to ease the NAS administration job.
  - Volume Manager: Responsible for volume management. Configuration of volume groups, logical volumes, volume snapshot and volume replication.
  - Raid Manager: For management and configuration of RAID controller
  - FC Target Manager: For setup of Fibre Channel Target volumes
  - iSCSI Target Manager: For setup of iSCSI Target volumes
  - Account Manager: Local and external account configuration. Import large accounts.
  - Backup Manager: Supports system configuration backup and setup the backup plan for data backup.
  - Share Manager: Share configuration and ACL setting. This also includes Rsync and Duplication functions.
  - System Manager: System configuration and firmware upgrade
  - Network Manager: Configuration of network information and NIC trunking.
  - Log Manager: Contains NAS system logs.
  - Event Manager: Configuration of email notification and system actions when events occur.
- **File Manager**: Provides user logon mode for share owner to perform folder and file management such as share folder access control.
- **proNAS HA**: (optional). Provides function of High Availability (two-node cluster) in Active-Standby mode.
- **proBackup**: Provides web-based GUI backup solution for desktop clients.

Each function of these components is described in the following Chapters.

NOTE: Some pictures and screenshots might be different from the actual NAS machine.

4.2 Installation and Configuration Phases

The installation and configuration of a proNAS system can be divided into five phases.

Phase 1: Set up the Hardware RAID Controller and create Raid Set.

Prior to proNAS system configuration, a basic hardware RAID configuration must be setup. Please refer to Section 4.4 for the basic setup instructions in creating Raid Set using Raid Manager. Refer to Section 4.5 for detailed information about Raid Manager.

Phase 2: Configure proNAS and its components with proNAS Manager. This is described in details in Chapter 5 proNAS Manager. To configure proNAS, you need to:

- Join a disk device (Raid Set, example: RAID00), such as /dev/sdb, to the system default volume group "proNASVG" using Volume Manager. This is described in Chapter 5 Section 5.1.1 and 5.1.2.
- Configure the network settings via Network Manager. This is described in Chapter 5 Section 5.4.1.
- Create or import accounts with Account Manager as described in Chapter 5 Section 5.5.
- Setup the shares using Share Manager and assign account/group permissions. This is described in Chapter 5 Section 5.6.
- Windows clients can start using the proNAS shares using CIFS protocol. UNIX/Linux clients need to enable NFS protocol (disabled by default).
- Setup FC target Volumes or iSCSI target volumes. This is described in Sections 5.2 and 5.3 respectively.

Phase 3: Perform NAS system maintenance.

- Maintain system via System Manager, as described in Chapter 5 Section 5.7
- Check system status using Log Manager and Event Manager. This is described in Chapter 5 Sections 5.9 and 5.10.
- Backup system configuration and data using Backup Manager. This is described in Chapter 5 Section 5.8.

Phase 4: (Optional) Setup proNAS HA for high-availability environment. Please refer to Chapter 8 for proNAS HA configuration.

Phase 5: Users can store and backup data into proNAS system.

- Store data into proNAS system using File Manager, as described in Chapter 6.
- Backup data into proNAS system using proBackup, as described in Chapter 7.

4.3 Setting proNAS IP Address and Connecting to NAS Management GUI

NOTE: Java 2 Runtime Environment (J2RE) 1.4.2 or later must be installed before using the proNAS management GUI. (Free download from: http://java.sun.com/j2se/index.jsp)

1. If necessary, reconfigure the network settings of your client computer to be able to connect to LAN0 IP address 172.16.0.1 (see table below), or add IP address 172.16.0.5 subnet 255.255.0.0.

Entity	Default Value
LAN0 IP address	172.16.0.1
Subnet Mask	255.255.0.0
Hostname	proNAS
Username	admin
Password	proware

NAS Default Values

2. To connect to NAS management GUI, open Web browser.
3. Enter the following URL in the address bar: http://172.16.0.1 then press Enter.
4. In the page that opens, click “Admin Login” button to enter the NAS management GUI.

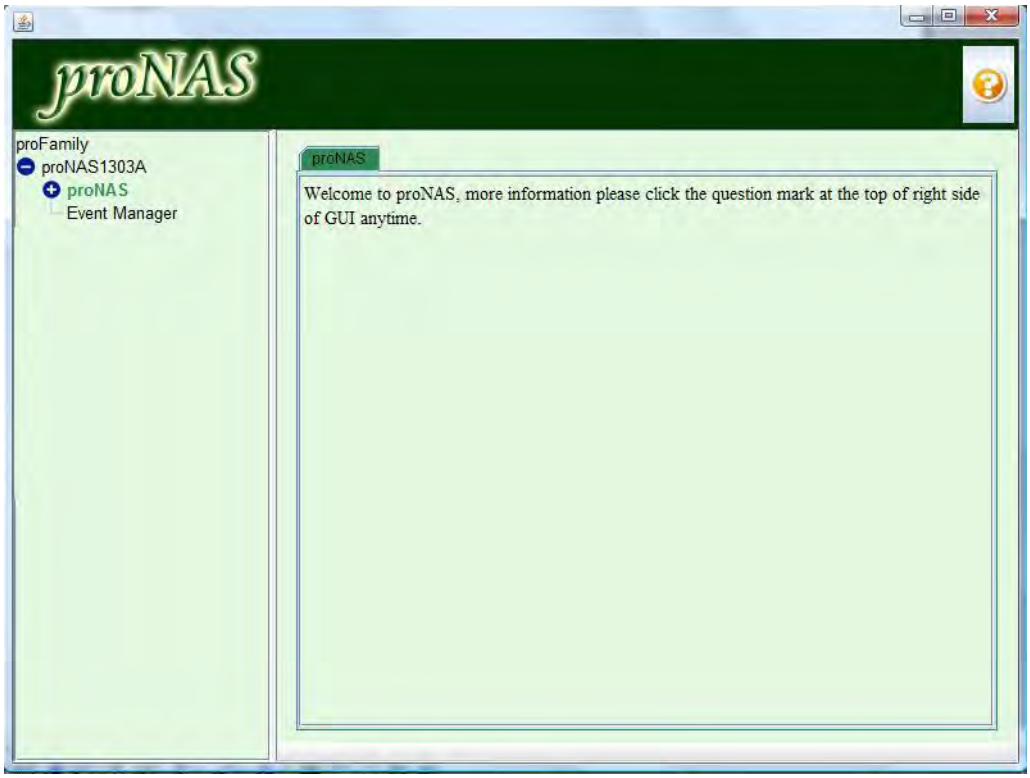
START button on the first proNAS

5. Enter Account as “admin” and password as “proware” and click the Logon button.

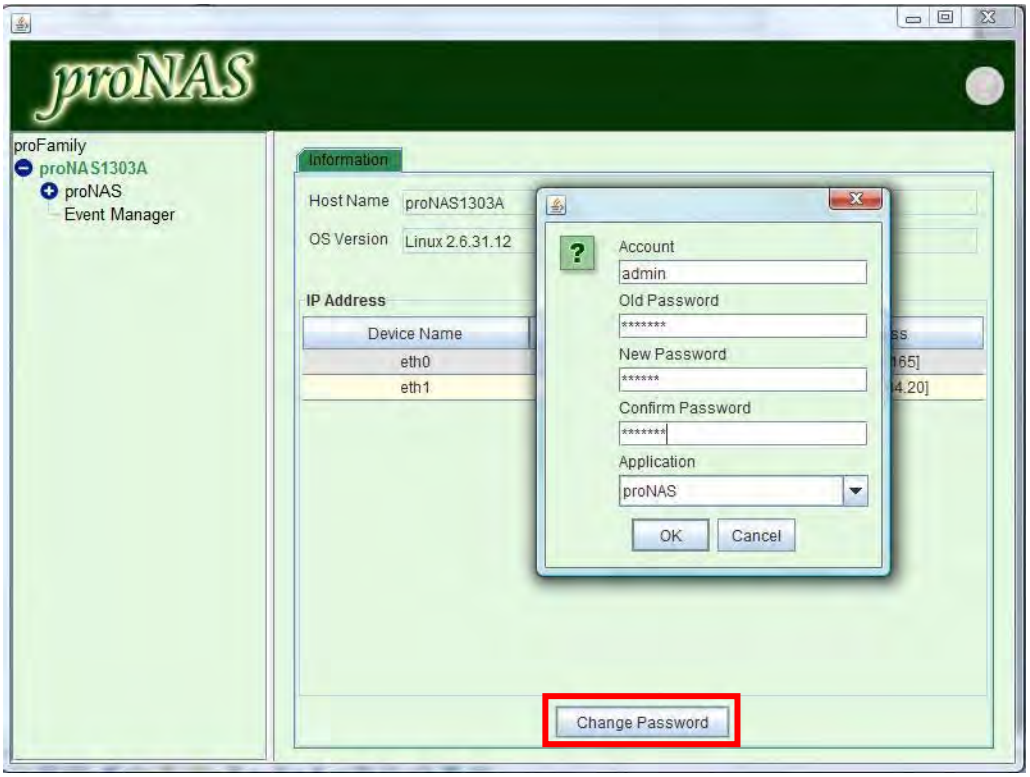
Login Screen

NOTE: proNAS supports language options: English, Chinese (Taiwan), Chinese (China), Japanese, Korean, German (Germany), Polish (Poland), and Russian (Russia). You can select your preferred language before logon.

6. The proNAS Manager main screen will be displayed showing proNAS and Event Manager.



NOTE: For security reason, it is necessary to change the default proNAS admin password. To change admin password, click the "Change Password" button. Enter the Account name (admin), the old password, the new password, re-enter new password.



4.4 Basic Steps in Creating Raid Set Using Raid Manager

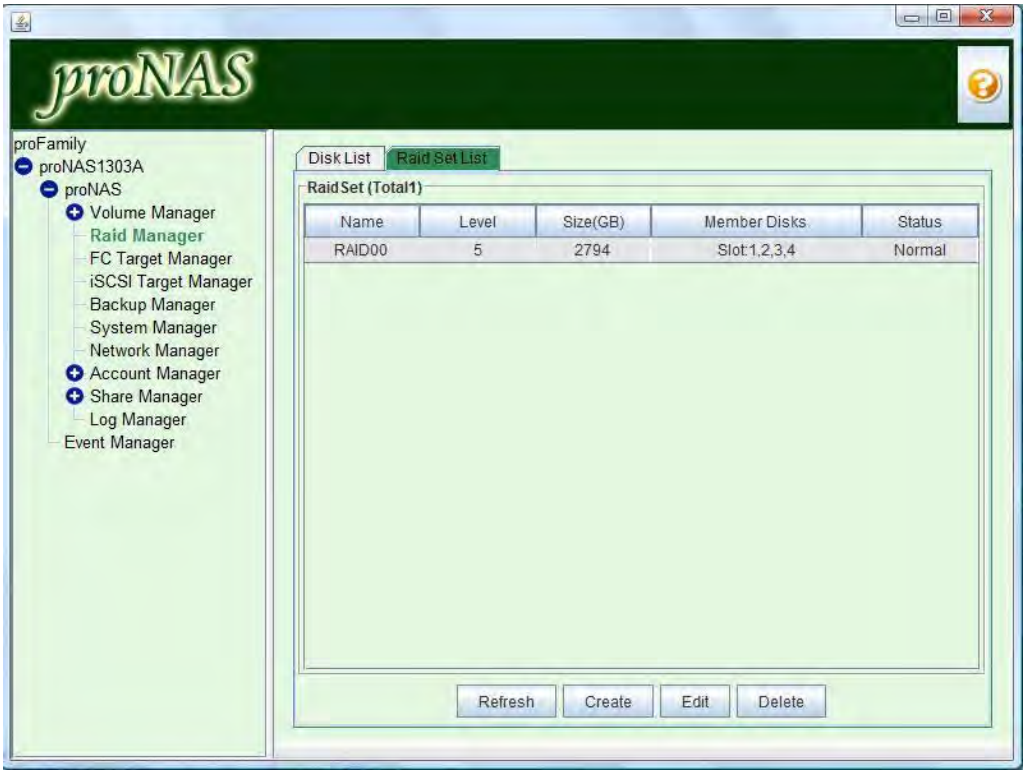
NOTE: If you have already created a Raid Set, you may skip this section.

This example creates a single Raid Set using 4 disk drives, RAID Level 5, quick initialization, and has over 2TB capacity.

1. Login to proNAS java GUI, if not yet logged in.

2. Select Raid Manager.

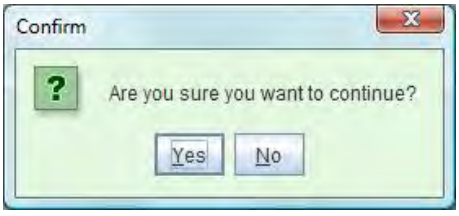
3. Select “Raid Set List” tab. Then click “Create”.

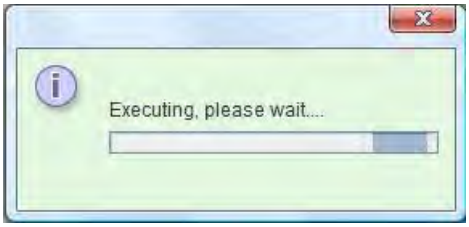


4. Select the disk drives to be included in the Raid Set. Select/change the RAID Level, if necessary. Click “OK” button when done.

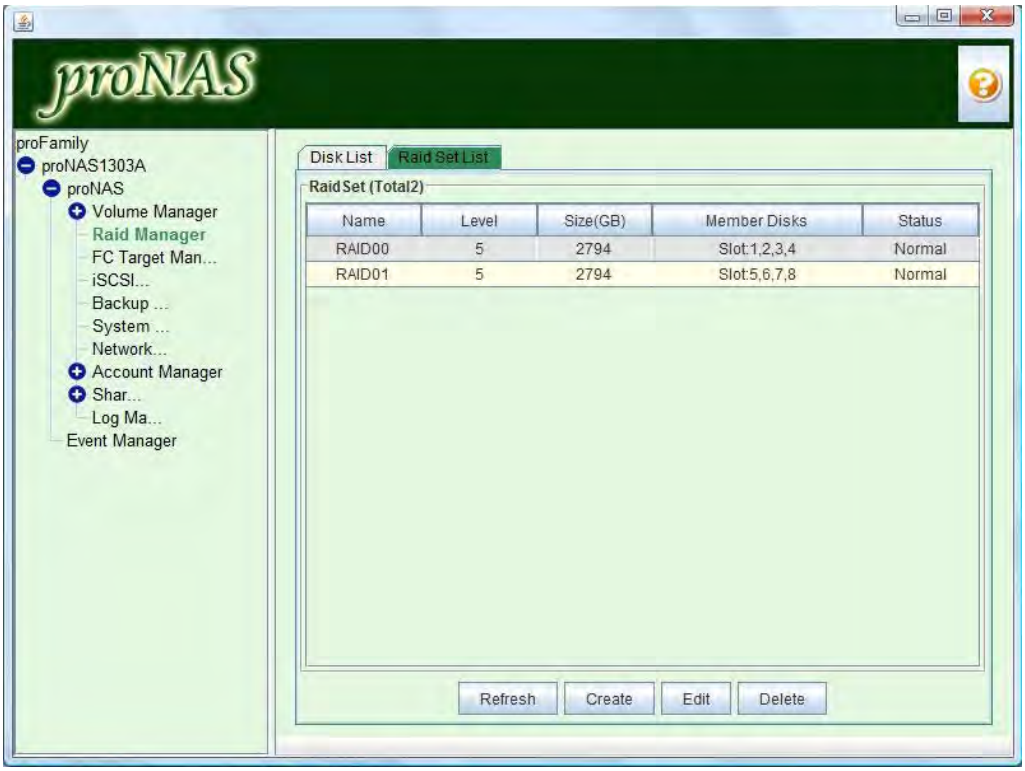
NOTE: The default Raid Set Name for first Raid Set is “RAID00”. The Quick Initialize option is selected by default, which means the Raid Set (RAID disk) will be quickly initialized and the Status will show “Normal”. If this option is disabled, the Raid Set will go through the initialization process and Status will show the percentage of initialization done until finished.

5. Click “Yes” to confirm.





6. The Raid Set will be created and shown in Raid Set List. The Status will show Normal.



7. The NAS system will be able to detect the newly created Raid Set (RAID disk device), such as /dev/sdc, in proNAS Volume Manager. If the disk device is not shown, click “Refresh” button in Volume Manager.

NOTE: The NAS system will be able to detect the new Raid Set (RAID disk device) without needing to reboot the NAS system.

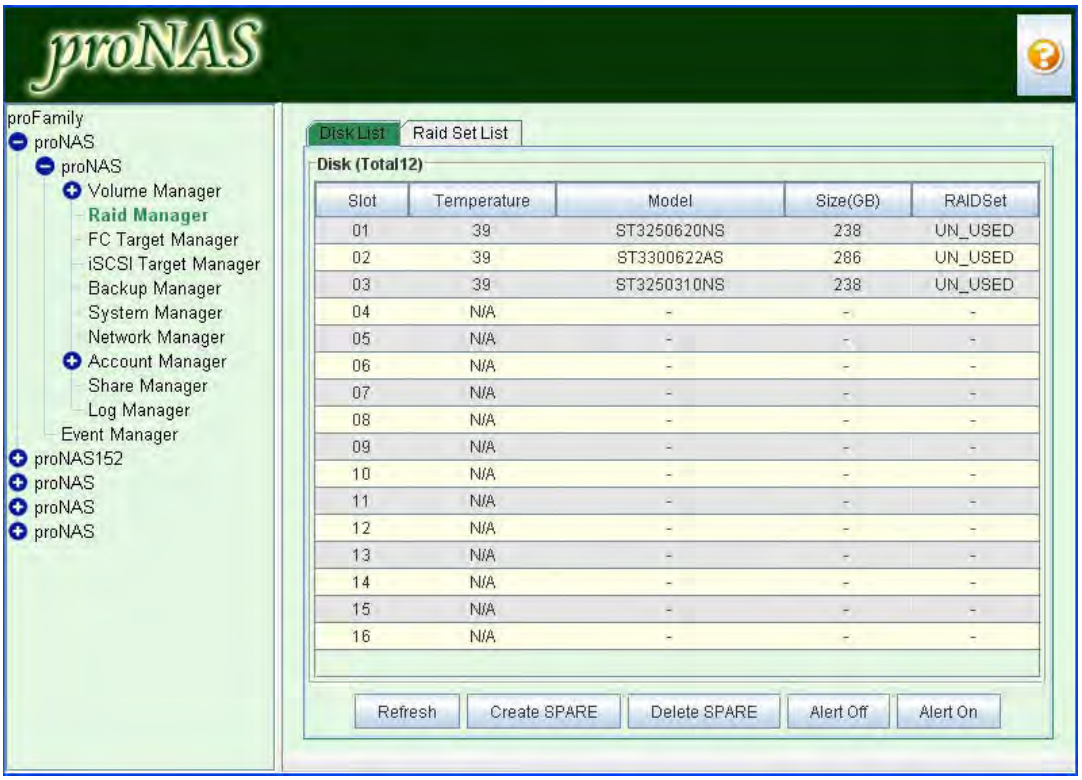
4.5 Raid Manager

4.5.1 Using Raid Manager

The Raid Manager provides the function to configure the RAID controller.

1. After login to proNAS java GUI, the Raid Manager will be available under the proNAS node. If the proNAS nodes (sub-menus) are not shown, click the "+" sign to display the nodes or sub-menus under it.

   The default tab in Raid Manager is the Disk List.


proNAS
proFamily
proNAS
proNAS
Volume Manager
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS152
proNAS
proNAS
proNAS
Disk List
Raid Set List
Disk (Total12)
Slot | Temperature | Model | Size(GB) | RAIDSet
01 | 39 | ST3250620NS | 238 | UN_USED
02 | 39 | ST3300622AS | 286 | UN_USED
03 | 39 | ST3250310NS | 238 | UN_USED
04 | N/A | - | - | -
05 | N/A | - | - | -
06 | N/A | - | - | -
07 | N/A | - | - | -
08 | N/A | - | - | -
09 | N/A | - | - | -
10 | N/A | - | - | -
11 | N/A | - | - | -
12 | N/A | - | - | -
13 | N/A | - | - | -
14 | N/A | - | - | -
15 | N/A | - | - | -
16 | N/A | - | - | -
Refresh
Create SPARE
Delete SPARE
Alert Off
Alert On

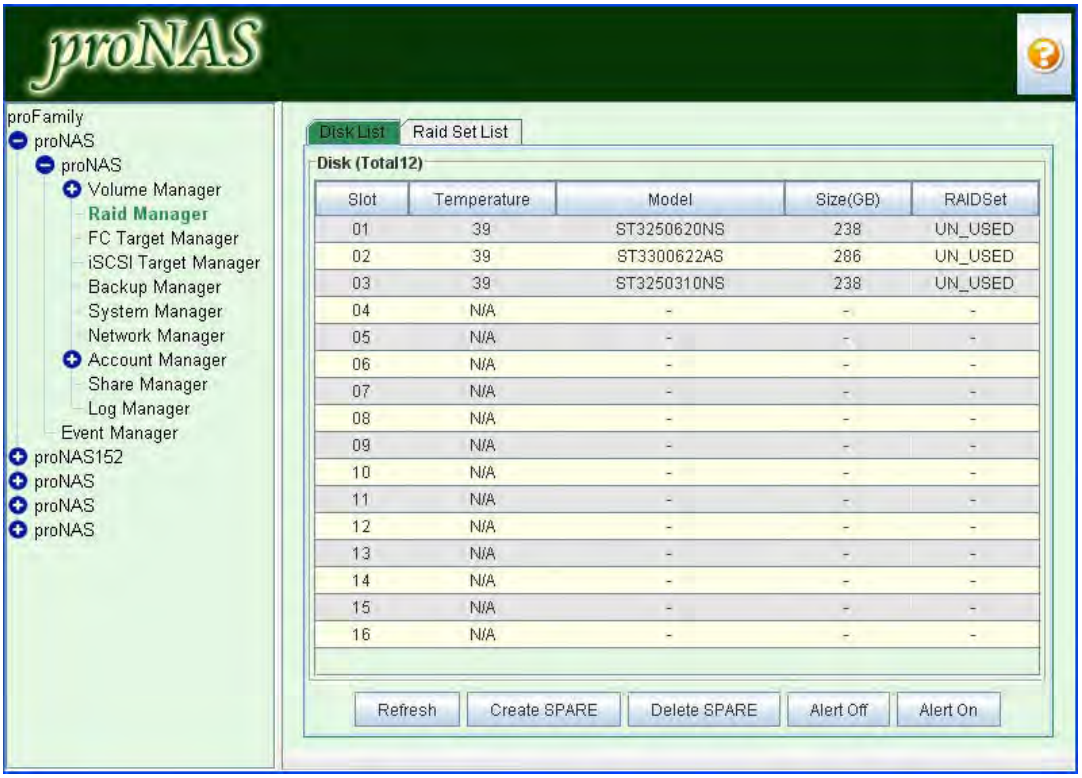
Disk List

2. To show the Raid Set List, click the “Raid Set List” tab.

Raid Set List

4.5.2 Disk List

The Disk List shows the list of disk drives in the NAS system. A hot spare drive can also be configured here.


proNAS
proFamily
proNAS
proNAS
Volume Manager
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS152
proNAS
proNAS
proNAS
Disk List
Raid Set List
Disk (Total12)
Slot | Temperature | Model | Size(GB) | RAIDSet
01 | 39 | ST3250620NS | 238 | UN_USED
02 | 39 | ST3300622AS | 286 | UN_USED
03 | 39 | ST3250310NS | 238 | UN_USED
04 | N/A | - | - | -
05 | N/A | - | - | -
06 | N/A | - | - | -
07 | N/A | - | - | -
08 | N/A | - | - | -
09 | N/A | - | - | -
10 | N/A | - | - | -
11 | N/A | - | - | -
12 | N/A | - | - | -
13 | N/A | - | - | -
14 | N/A | - | - | -
15 | N/A | - | - | -
16 | N/A | - | - | -
Refresh
Create SPARE
Delete SPARE
Alert Off
Alert On

Buttons	Function
Refresh	Use this to update the information shown in the proNAS GUI.
Create SPARE	Use this to create a hot spare disk.
Delete SPARE	Use this to delete a hot spare disk. The disk will become a Free or UN_USED disk.
Alert Off	Use this to disable the alarm beeper.
Alert On	Use this to enable the alarm beeper.

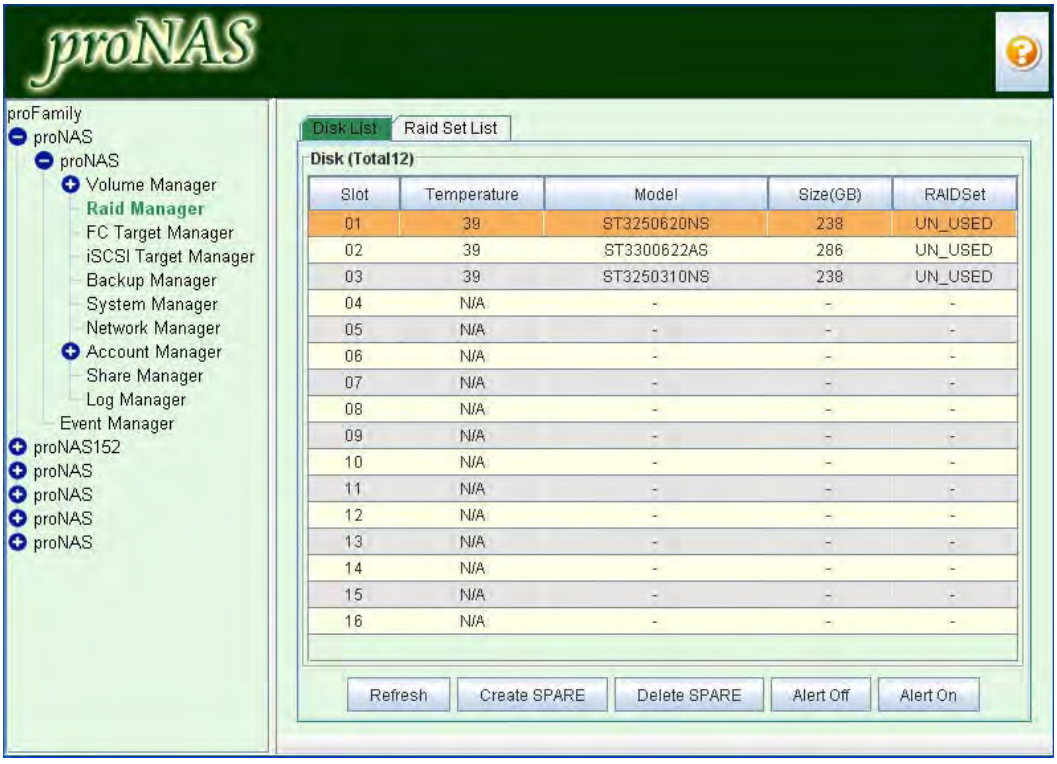
4.5.2.1 Create Hot Spare Disk

NOTE: The Hot Spare Disk must have same (equal) or bigger capacity as the disk it will automatically replace. If the capacity is smaller, it will not be able to replace a failed disk drive, and the Raid Set will not be rebuilt.

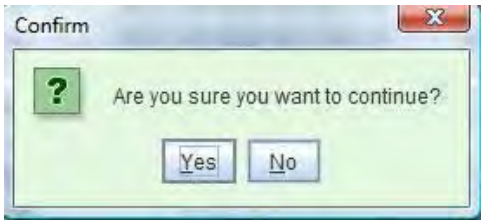
To create a Hot Spare Disk:

1. Select Raid Manager.

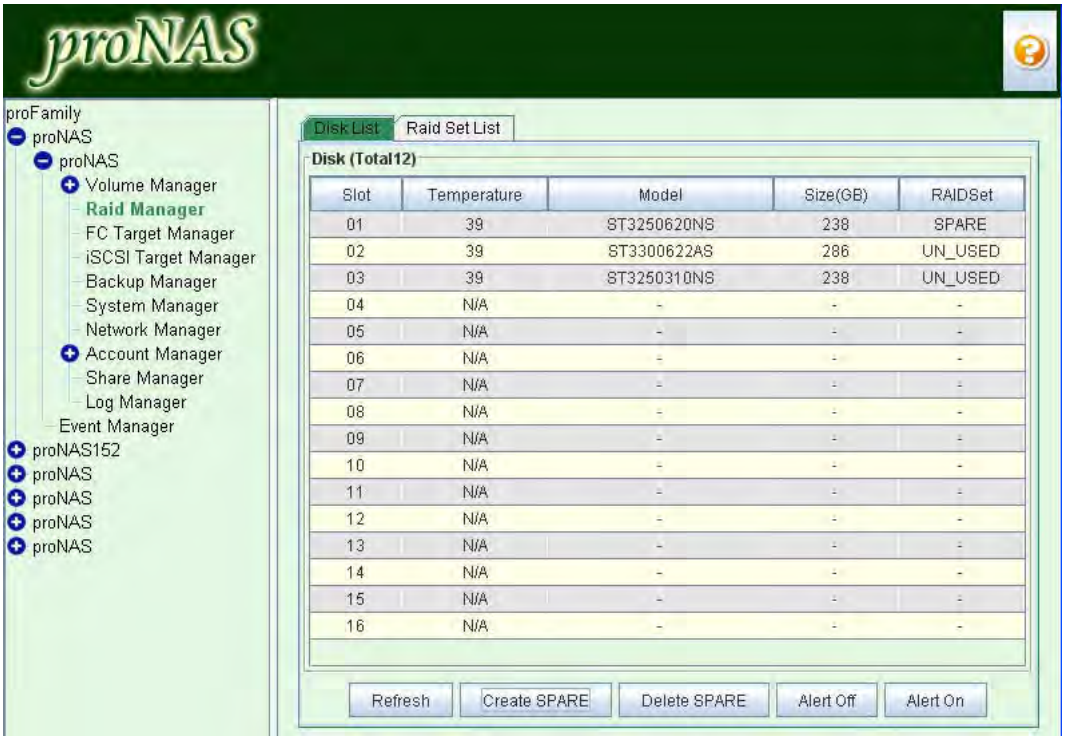
2. While in Disk List tab, select an UN_USED disk from the list of disk drives. The disk drive will be highlighted.


proNAS
proFamily
proNAS
proNAS
Volume Manager
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS152
proNAS
proNAS
proNAS
proNAS
Disk List
Raid Set List
Disk (Total12)
Slot | Temperature | Model | Size(GB) | RAIDSet
01 | 39 | ST3250620NS | 238 | UN_USED
02 | 39 | ST3300622AS | 286 | UN_USED
03 | 39 | ST3250310NS | 238 | UN_USED
04 | N/A | - | - | -
05 | N/A | - | - | -
06 | N/A | - | - | -
07 | N/A | - | - | -
08 | N/A | - | - | -
09 | N/A | - | - | -
10 | N/A | - | - | -
11 | N/A | - | - | -
12 | N/A | - | - | -
13 | N/A | - | - | -
14 | N/A | - | - | -
15 | N/A | - | - | -
16 | N/A | - | - | -
Refresh
Create SPARE
Delete SPARE
Alert Off
Alert On

3. Click the “Create SPARE” button. A confirmation message will be displayed. Click “Yes”.



4. The selected disk drive will become a Hot Spare drive.

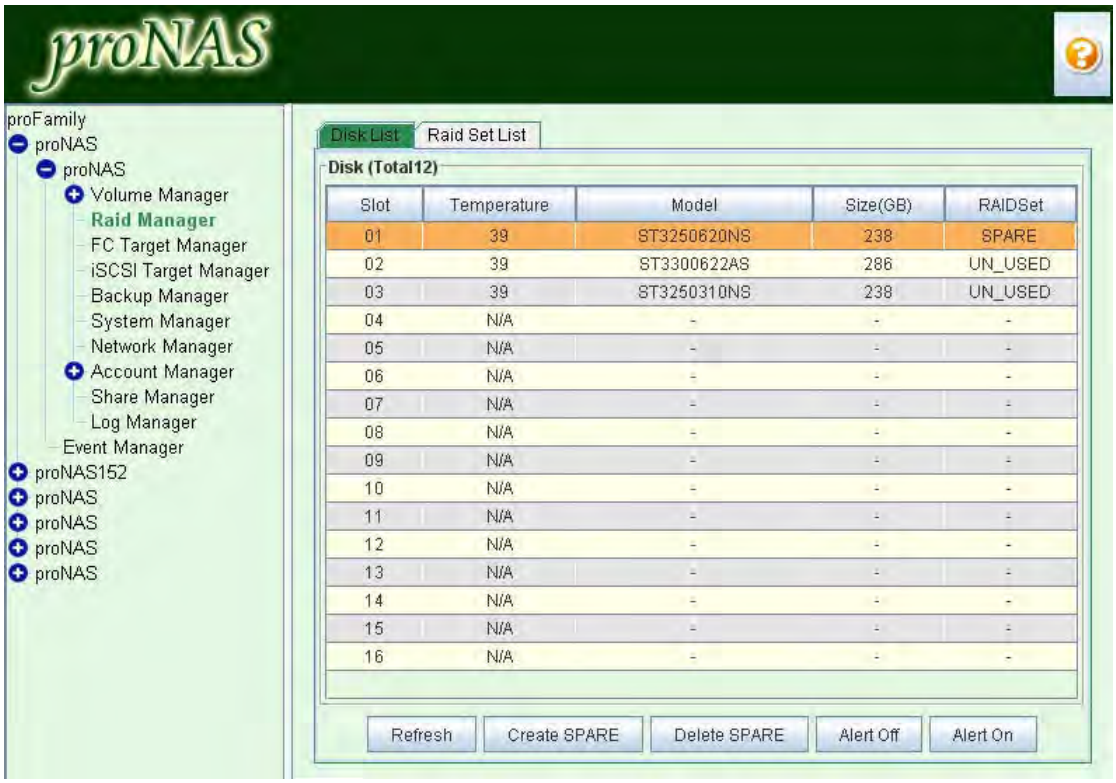


4.5.2.2 Delete Hot Spare

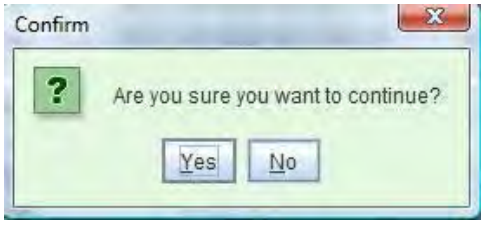
To delete a Hot Spare Disk and make it a “free” or UN_USED disk drive:

1. Select Raid Manager.

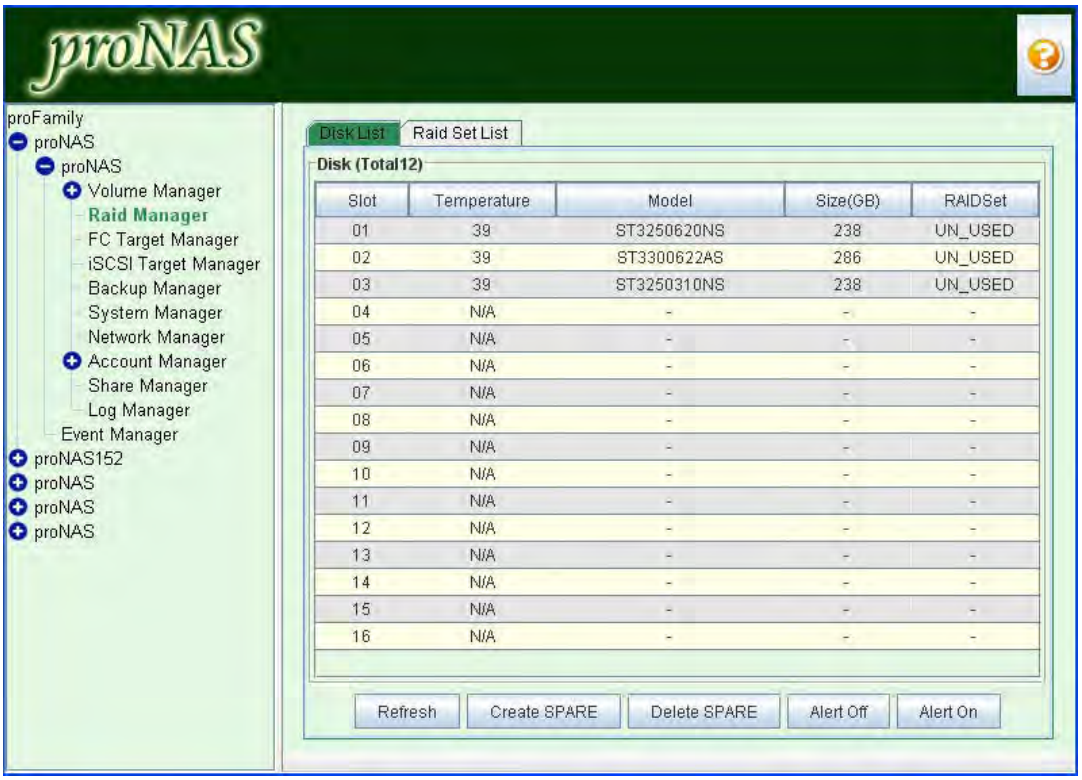
2. While in Disk List tab, select the SPARE disk that will be made a free disk. The disk drive will be highlighted.


proNAS
proFamily
proNAS
proNAS
Volume Manager
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS152
proNAS
proNAS
proNAS
proNAS
Disk List
Raid Set List
Disk (Total12)
Slot | Temperature | Model | Size(GB) | RAIDSet
01 | 39 | ST3250620NS | 238 | SPARE
02 | 39 | ST3300622AS | 286 | UN_USED
03 | 39 | ST3250310NS | 238 | UN_USED
04 | N/A | - | - | -
05 | N/A | - | - | -
06 | N/A | - | - | -
07 | N/A | - | - | -
08 | N/A | - | - | -
09 | N/A | - | - | -
10 | N/A | - | - | -
11 | N/A | - | - | -
12 | N/A | - | - | -
13 | N/A | - | - | -
14 | N/A | - | - | -
15 | N/A | - | - | -
16 | N/A | - | - | -
Refresh
Create SPARE
Delete SPARE
Alert Off
Alert On

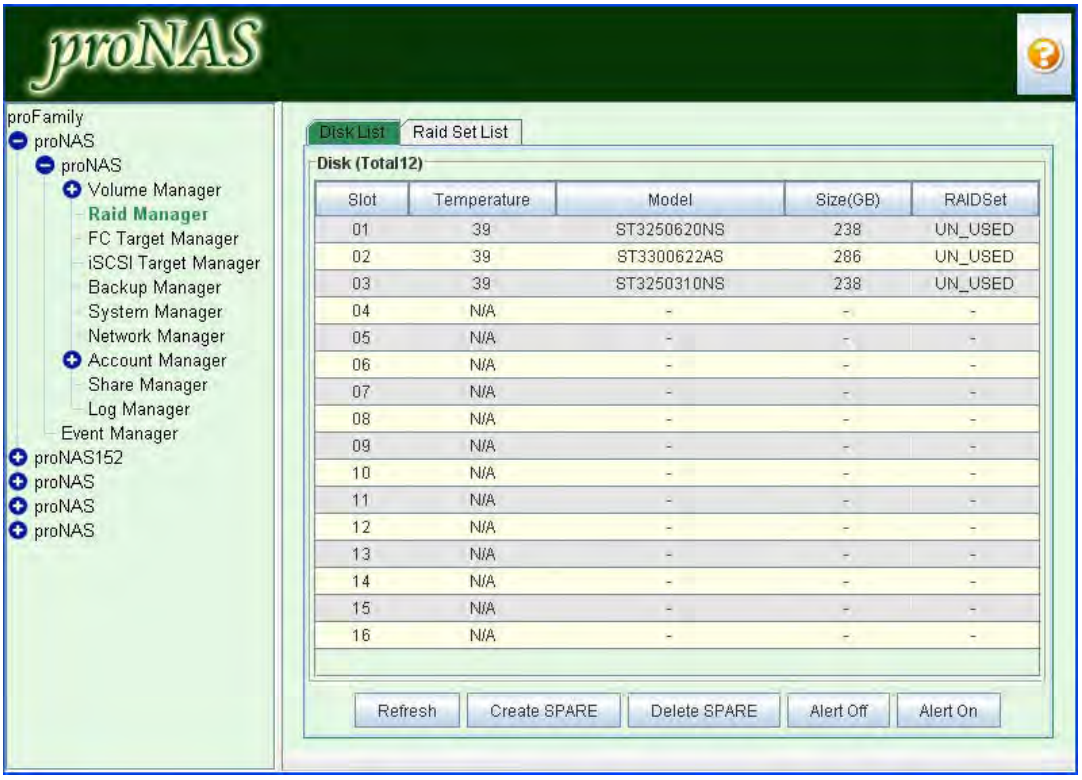
3. Click the “Delete SPARE” button. A confirmation message will be displayed. Click “Yes”.



4. The selected disk drive will become a free or UN_USED disk drive.


proNAS
proFamily
proNAS
proNAS
Volume Manager
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS152
proNAS
proNAS
proNAS
Disk List
Raid Set List
Disk (Total12)
Slot | Temperature | Model | Size(GB) | RAIDSet
01 | 39 | ST3250620NS | 238 | UN_USED
02 | 39 | ST3300622AS | 286 | UN_USED
03 | 39 | ST3250310NS | 238 | UN_USED
04 | N/A | - | - | -
05 | N/A | - | - | -
06 | N/A | - | - | -
07 | N/A | - | - | -
08 | N/A | - | - | -
09 | N/A | - | - | -
10 | N/A | - | - | -
11 | N/A | - | - | -
12 | N/A | - | - | -
13 | N/A | - | - | -
14 | N/A | - | - | -
15 | N/A | - | - | -
16 | N/A | - | - | -
Refresh
Create SPARE
Delete SPARE
Alert Off
Alert On

4.5.2.3 Alert Off / Alert On

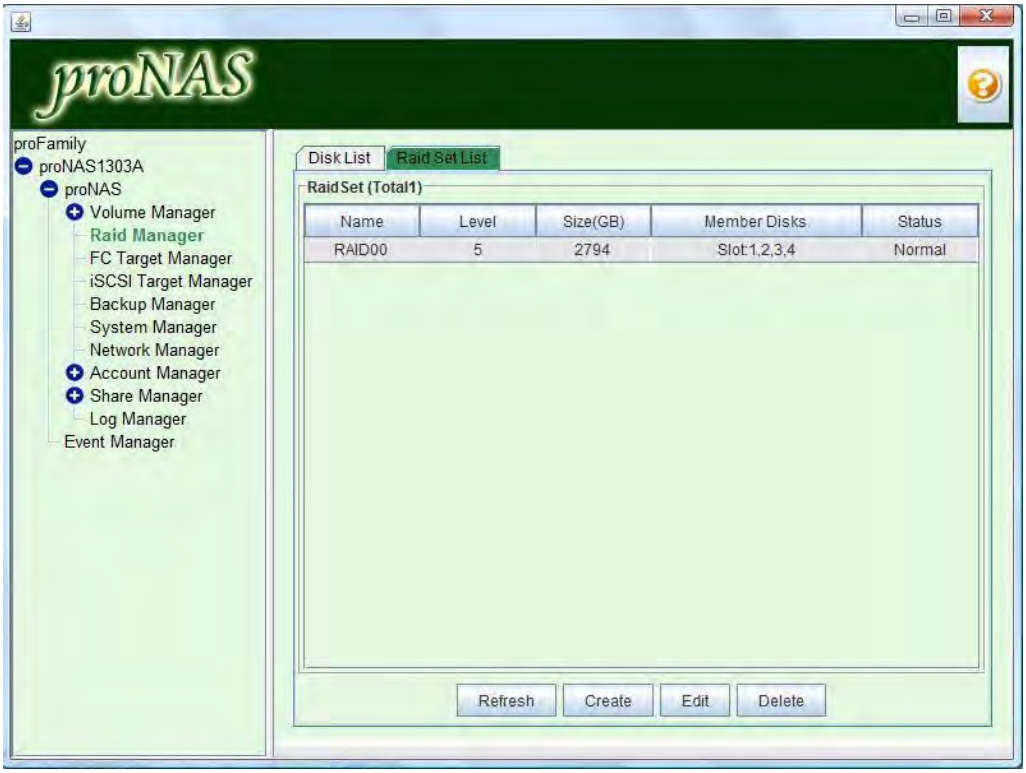


Alert Off – Use this to disable the alarm beeper. For example, if one disk drive failed and alarm beeper sounded, clicking this button will silent and disable the alarm beeper. If another event happens, the alarm beeper will not sound (always disabled until enabled).

Alert On – Use this to enable the alarm beeper.

4.5.3 Raid Set List

The Raid Set List shows the list of Raid Sets in the NAS system. A Raid Set can also be created, modified, or deleted here.



Buttons	Function
Refresh	Use this to update the information shown in the proNAS GUI.
Create	Use this to create a Raid Set.
Edit	Use this to modify an existing Raid Set.
Delete	Use this delete an existing Raid Set.

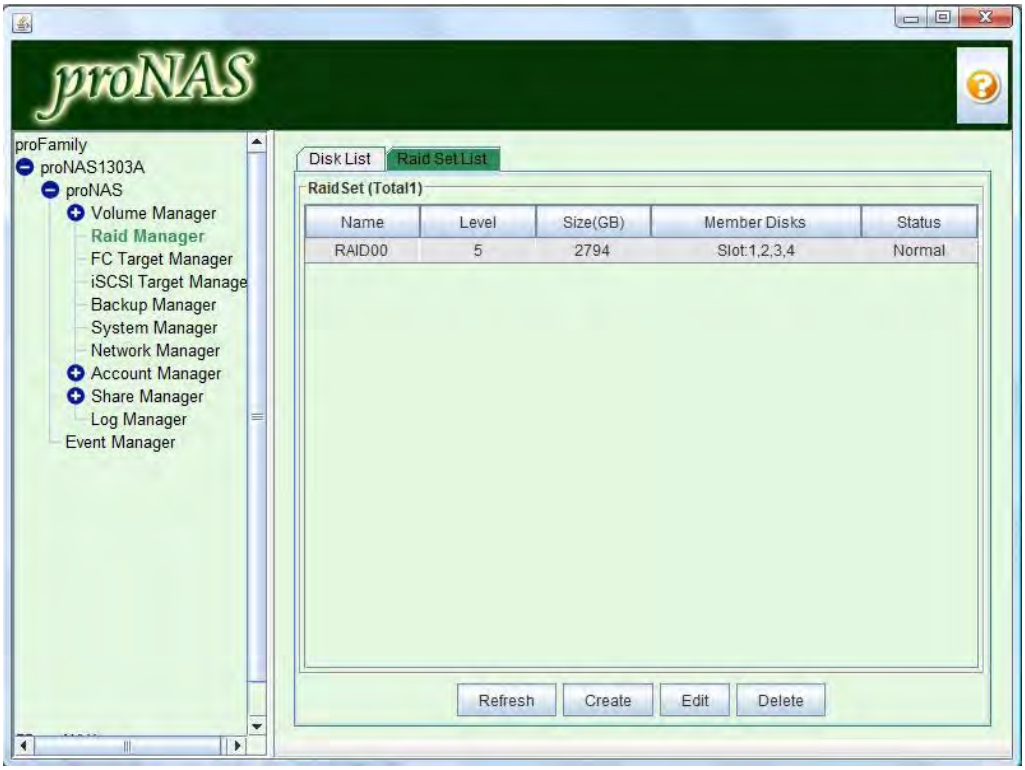
4.5.3.1 Create Raid Set

NOTE: A Raid Set (RAID disk device) will appear to the NAS system as a SCSI disk device (for example, /dev/sdb) which can be joined to proNAS Volume Group.

To create a Raid Set:

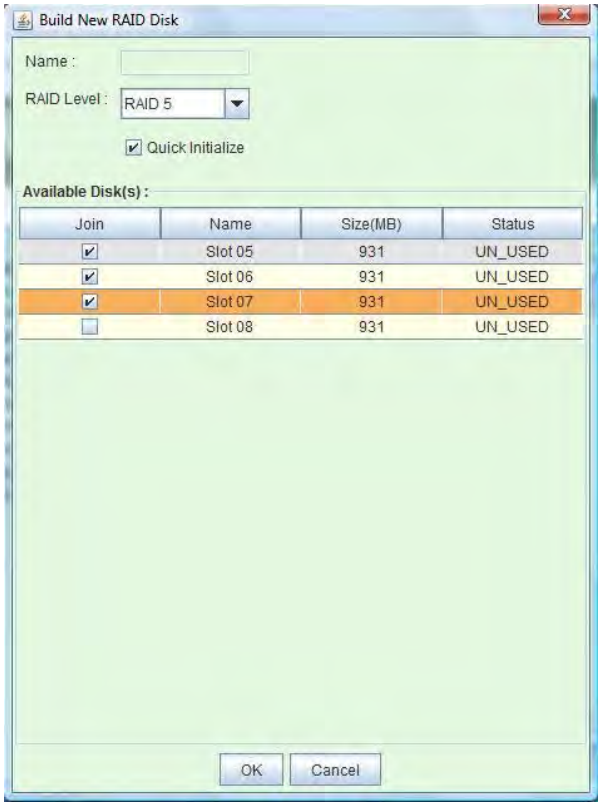
1. Select Raid Manager.

2. Select Raid Set List tab, and then click “Create” button.



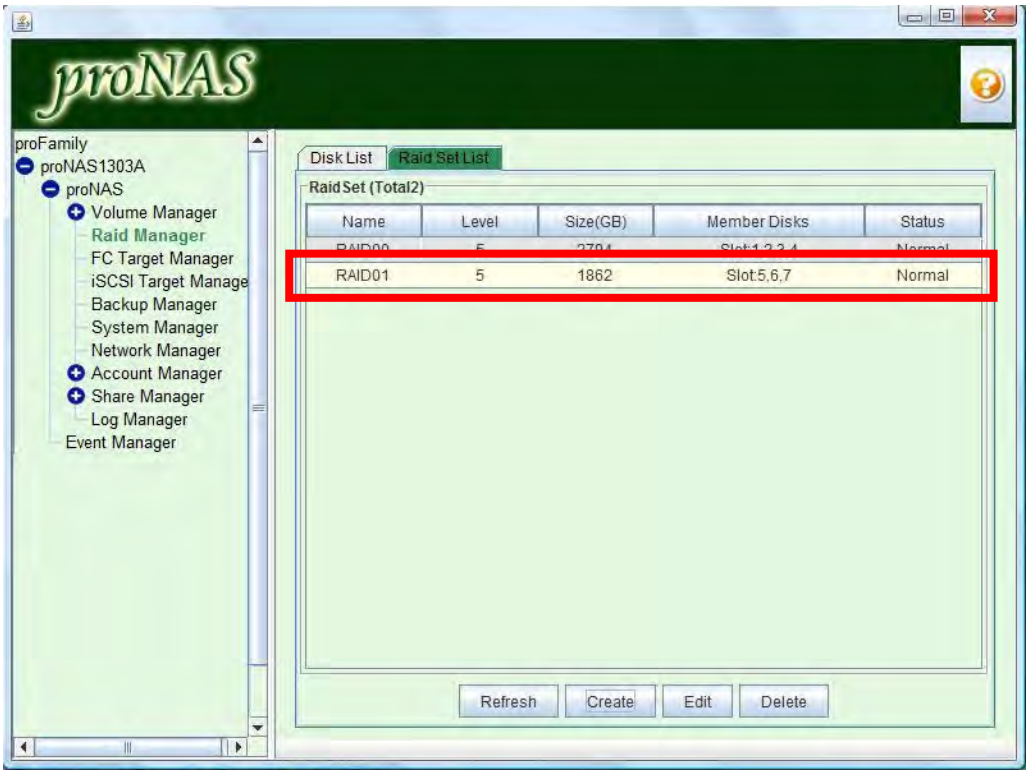
3. Select the disk drives to be included in the Raid Set. Select/change the RAID Level, if necessary. Click “OK” button when done.

NOTE: The default Raid Set Name for first Raid Set is “RAID00” and “RAID01” for the second Raid Set.
The Quick Initialize option is selected by default, which means the Raid Set (RAID disk) will be quickly initialized and the Status will show “Normal”. If this option is disabled, the Raid Set will go through the initialization process and Status will show the percentage of initialization done until finished.



4. Click “Yes” to confirm.

5. The Raid Set will be created and shown in Raid Set List. The Status will show Normal.



6. The NAS system will be able to detect the newly created Raid Set (RAID disk device), such as /dev/sdc, in proNAS Volume Manager. If the disk device is not shown, click “Refresh” button in Volume Manager.

NOTE: The NAS system will be able to detect the new Raid Set (RAID disk device) without needing to reboot the NAS system.

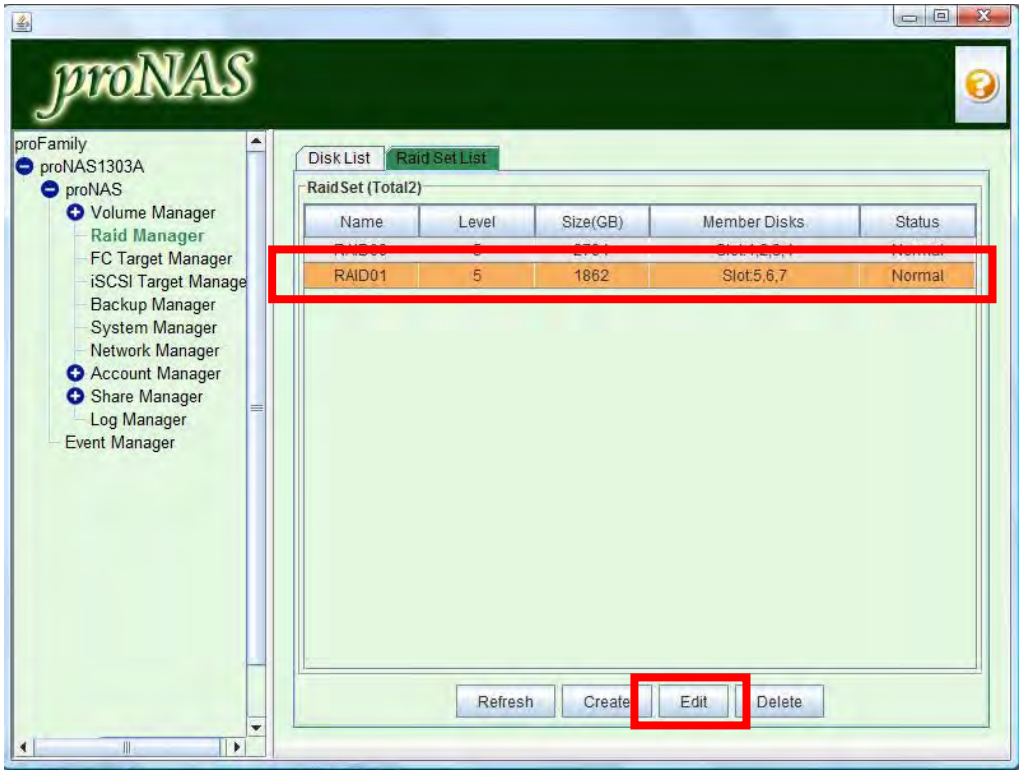
4.5.3.2 Edit Raid Set

An existing Raid Set can be modified, such as adding new disk drive(s) to expand the capacity of the Raid Set.

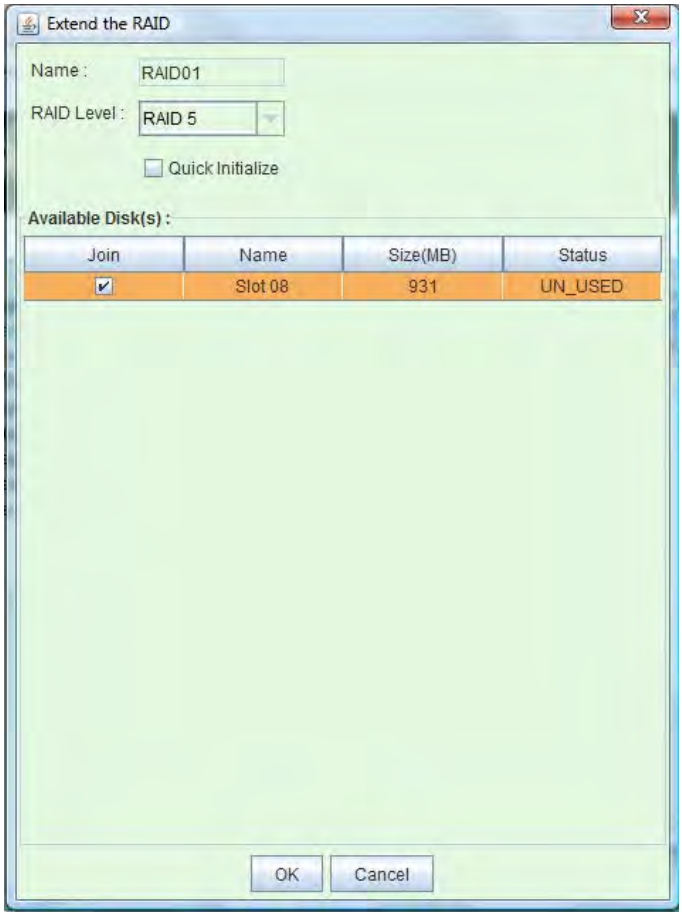
To modify/expand a Raid Set:

1. Select Raid Manager.

2. Select “Raid Set List” tab. Select the Raid Set (RAID01) that will be edited, and then click “Edit” button.

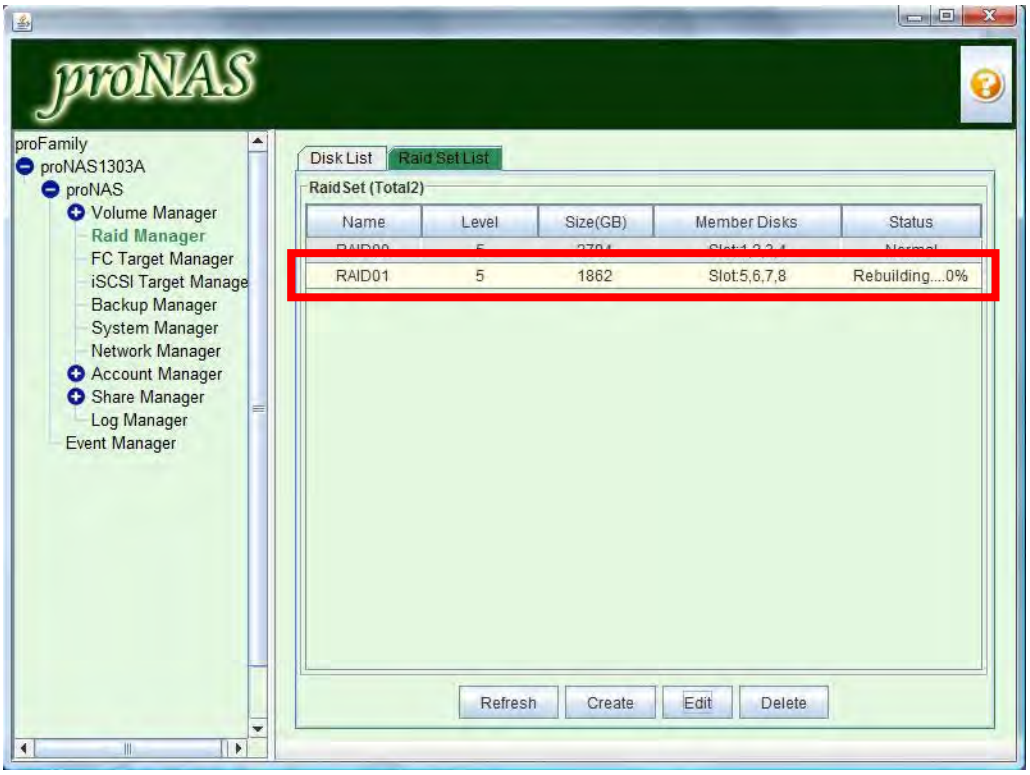


3. Select the disk drive(s) to be added in the Raid Set. Click “OK” button when done.



4. A confirmation message will be displayed. Click “Yes” to confirm.

5. The Raid Set will be expanded. The Status will show Rebuilding. Wait until the expansion process (Rebuilding) is done, then the Raid Set will show the extended capacity.



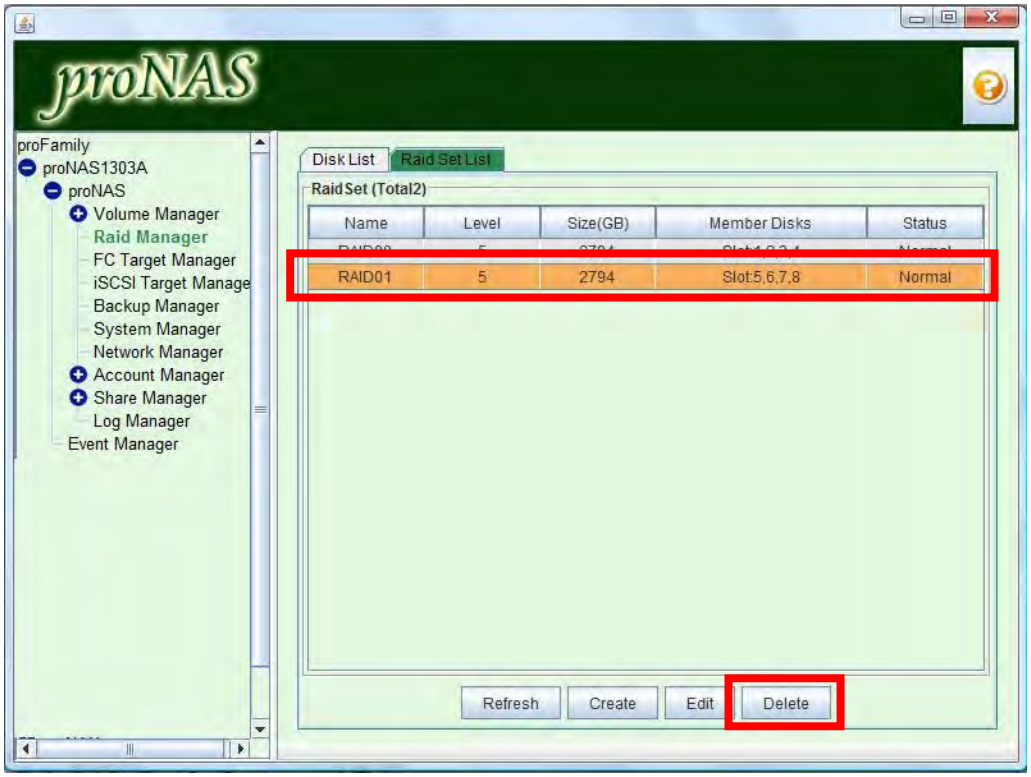
4.5.3.3 Delete Raid Set

NOTE: A Raid Set cannot be deleted if it is already joined to proNASVG in Volume Manager.
If a Raid Set is joined to another VG (not proNASVG), the other VG must be deleted first (existing volumes/shares of the VG will be deleted also) and then delete the Raid Set.

To delete a Raid Set:

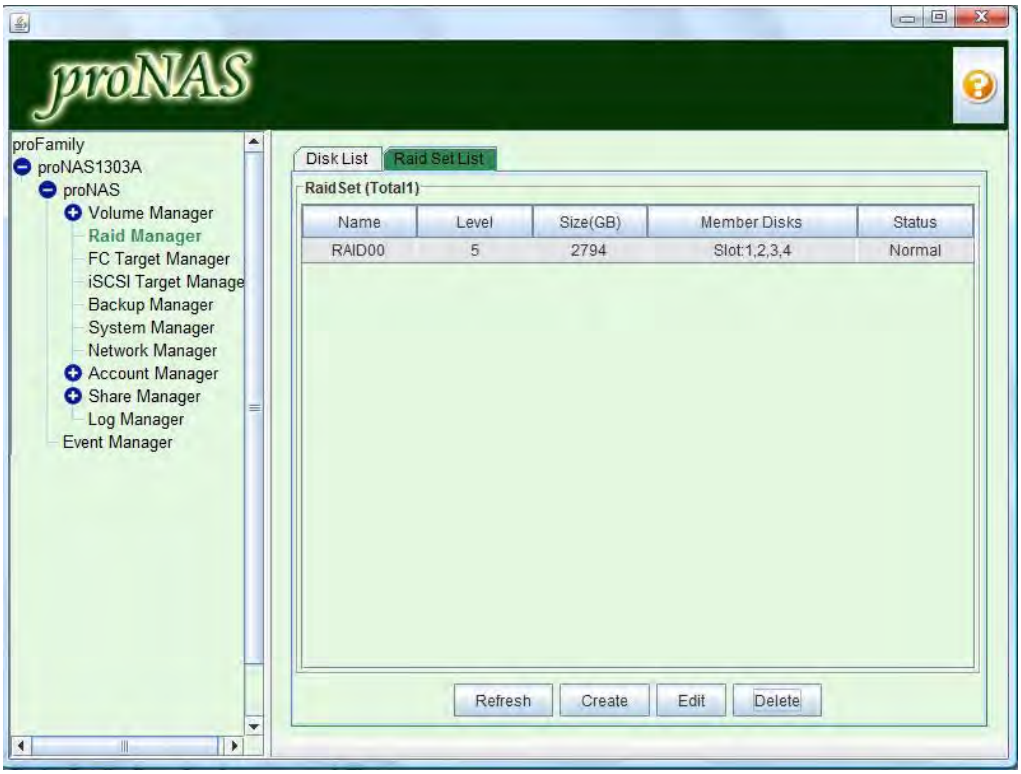
1. Select Raid Manager.

2. Select “Raid Set List” tab. Select the Raid Set (RAID01) that will be deleted, and then click “Delete” button.



3. A confirmation message will be displayed. Click “Yes” to confirm.

4. The Raid Set (RAID01) will be deleted.



Chapter 5 proNAS Manager

proNAS supports Multi-Node Management. If you have several NAS subsystems connected to the intranet, you can see all these systems when you login to the proNAS system. The IP Address section lists the NAS systems connected to the network. proNAS Multi-Node Technology is based on UDP Multi-Casting technology. The proNAS managers are listed below.

The proNAS managers are:

1. Volume Manager
2. FC Target Manager
3. iSCSI Target Manager
4. Network Manager
5. Account Manager
6. Share Manager
7. System Manager
8. Backup Manager
9. Log Manager
10. Event Manager

5.1 Volume Manager

The Volume Manager is responsible for disk and volume management.

A Volume Group consists of one or more disks that could be a RAID disk device or Raid Set created using Raid Manager. The default proNAS Volume Group (proNASVG) must be created first by joining at least one “New” or “Non_Initialized” disk to this volume group. The proNASVG holds the NAS system configuration and the default system Logical Volumes, such as home, public, proBackup Device, and proBackup Extended Device, as well as user-defined Logical Volumes. Files and folders reside on these Logical Volumes.

The default proNASVG Volume Group cannot be deleted. When proNASVG is created, the XFS file system is set in each default Logical Volume. XFS file system is also set in all user-defined Logical Volumes. XFS is a high performance journaling file system and provides better recovery time to repair a file system in case of FS damage. The proNAS Volume Group will dynamically allocate some space from its assigned disks, and allocation may fail if no more disk space is available. Therefore, make sure to regularly monitor the available free space of proNAS Volume Group.

The Volume Manager can perform the following function:

- Create a VG (volume group)
- Join New Disks
- Reset a VG (volume group)
- Remove a VG (volume group)
- Create Logical Volume
- Create Snapshot
- Create Replication

5.1.1 Volume Group Management

Volume Group (VG) is created by joining at least one disk device, which can be a Raid Set created in Raid Manager. Logical Volumes are created under the Volume Group.

proNASVG is the system default VG. It must be created (initialized) first in order to use the NAS system. To create the proNASVG, it is necessary to join at least one “New” or “Non_Initialized” disk into proNASVG.

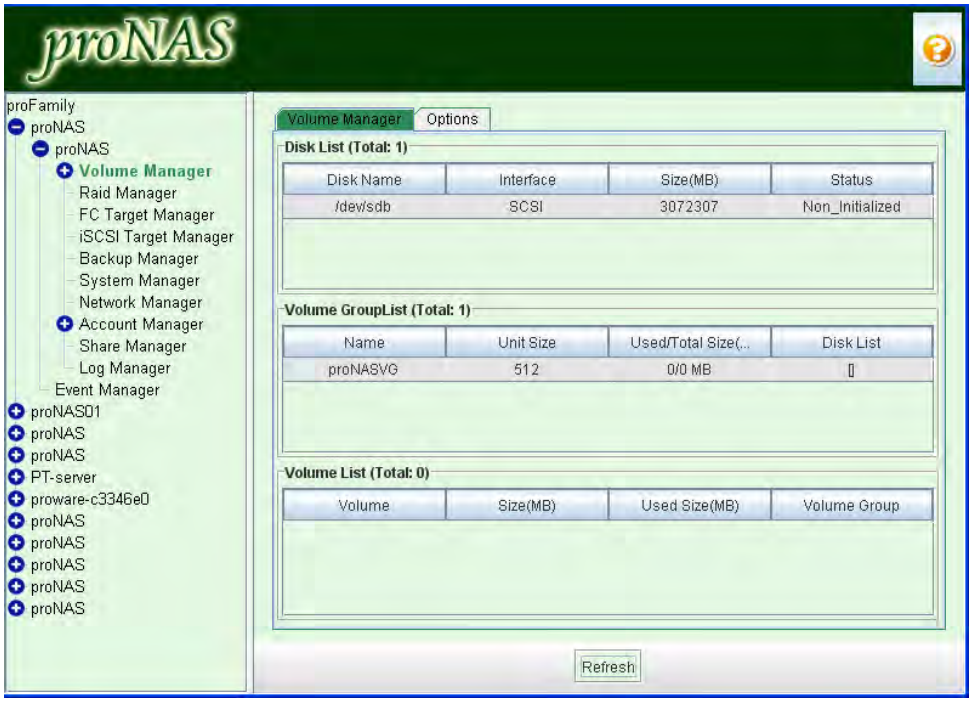
Admin can create other VG by joining other new or “Non_Initialized” disk, create or remove LV in this VG, join any new disk, remove any disk and reset the VG.

NOTE: The Raid Set created in Raid Manager will be detected in Volume Manager without needing to reboot the NAS system.

5.1.1.1 Create the proNASVG Volume Group

To create the proNASVG, perform the following steps:

1. Select Volume Manager. Verify that the Disk List shows at least one disk device (example: /dev/sdb) and the Status is “Non_Initialized’. Noticed in the Volume Group List that the proNASVG has no Disk List.

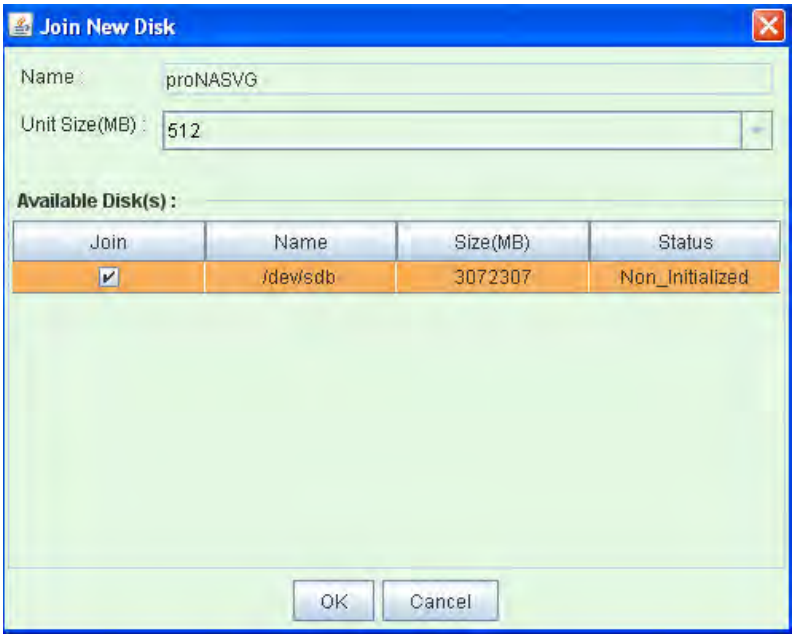


NOTE: The system default Volume Group “proNASVG” cannot be deleted or reset.

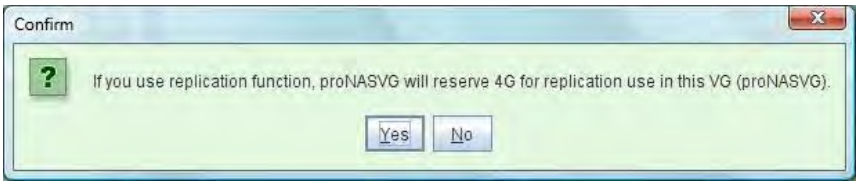
2. Select proNASVG under Volume Manager and click “Join New Disk” button.

3. Select the Disk(s) that will be joined to proNASVG from the list of Available Disk(s). Click “OK” when done.

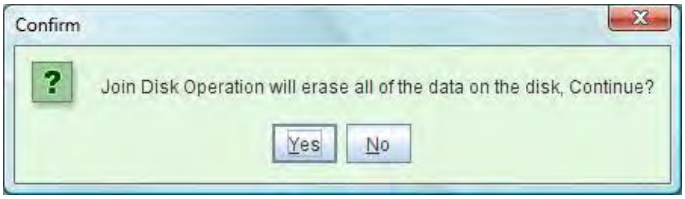
NOTE: Unit Size is the Physical Extent or block size used in the Volume Group. The VG Unit Size is set to 512MB and cannot be changed.



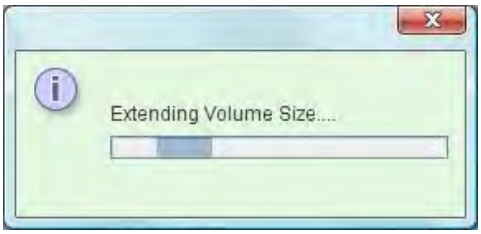
4. A confirmation message will appear. Select “Yes” to proceed.



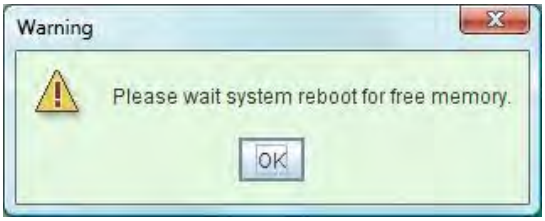
5. Another confirmation message will appear. Select “”Yes” to proceed.



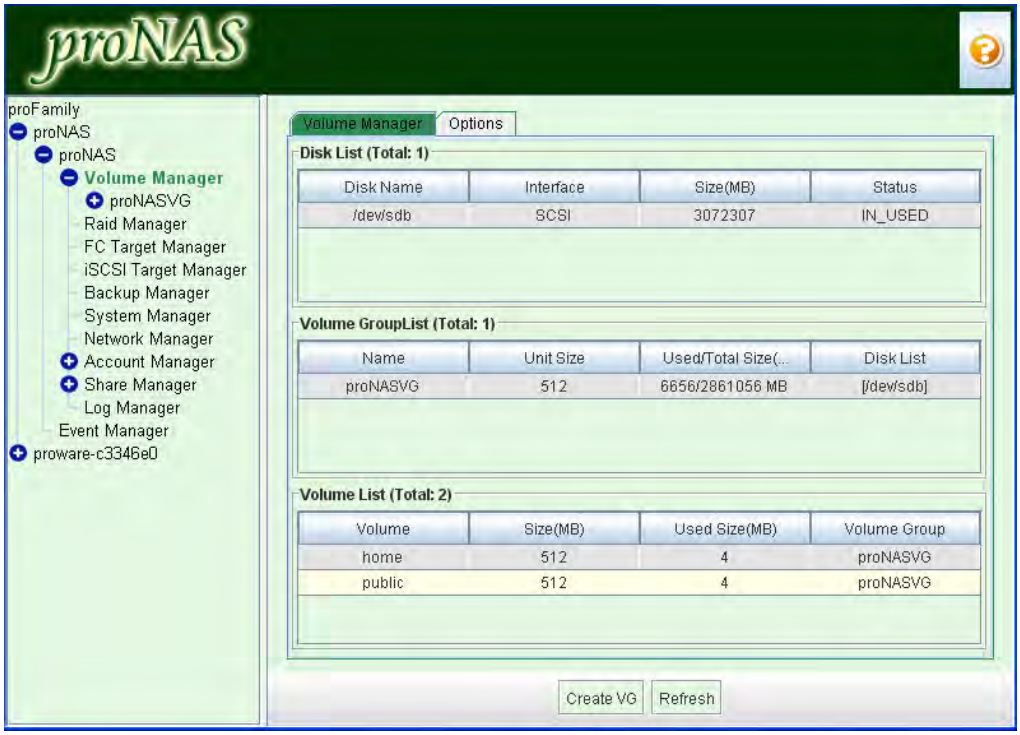
6. The process of joining disk to the VG will start.



7. When the process of joining disk to VG is completed, the NAS will reboot to free some used system memory. A warning message will be displayed. Click “OK” to close the message.



8. Wait for about 3 minutes then re-login to proNAS management GUI. The Volume Manager will show the joined disk as “IN_USED” and the Volume List will show the system default Logical Volumes “home” and “public”.



NOTE: The other system default Logical Volumes “proBackup Device” and “proBackup Extended Device” will only be created and become visible in the Volume List when the proBackup Service is started.

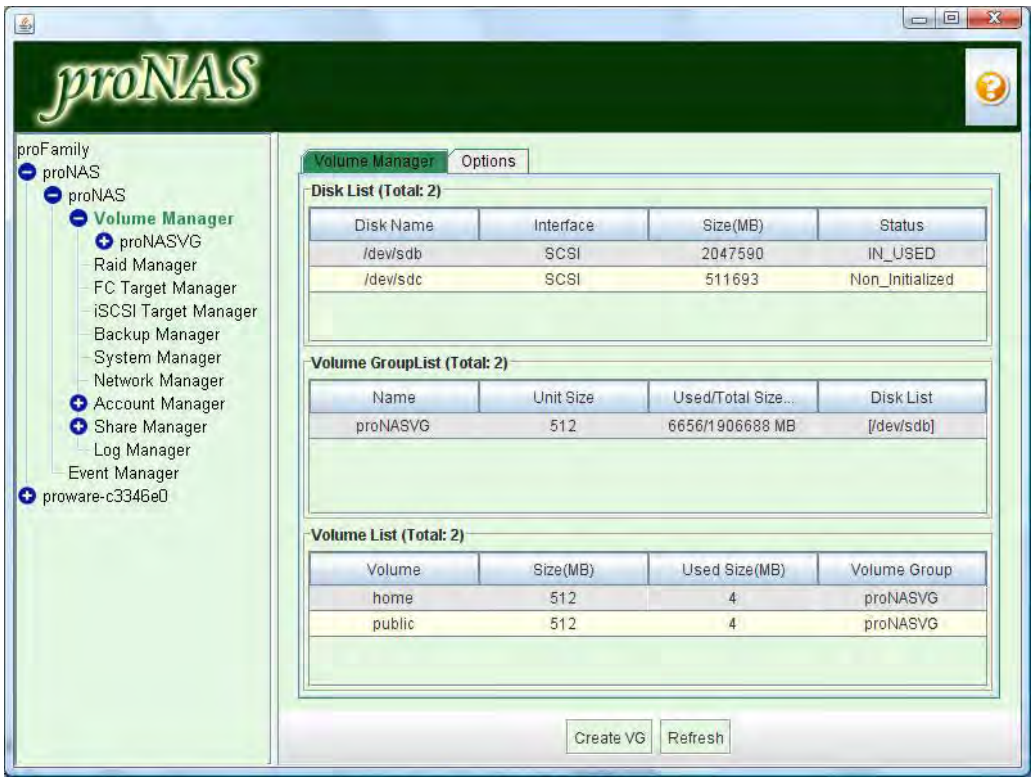
5.1.1.2 Creating another Volume Group

To create another VG, verify from Volume Manager Disk List if there is available free or “Non_Initialized” disk. If there is none, a new Raid Set (RAID disk device) must be created first.

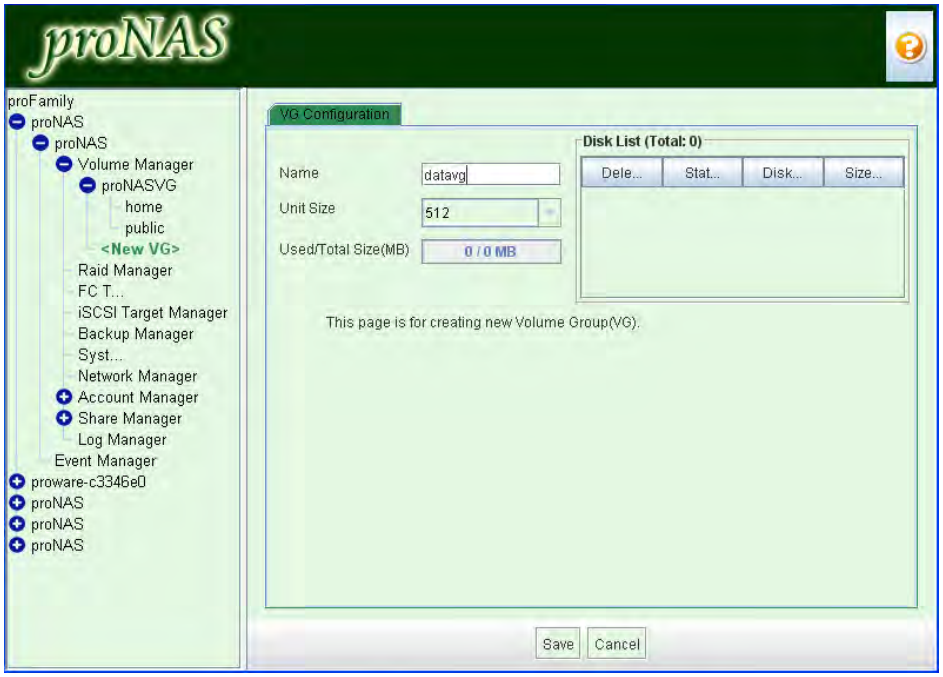
If a new Raid Set has already been created using Raid Manager, the Raid Set (disk device) will be automatically detected in Volume Manager.

To create another VG, perform the following steps:

1. In Volume Manager, click “Create VG” button.



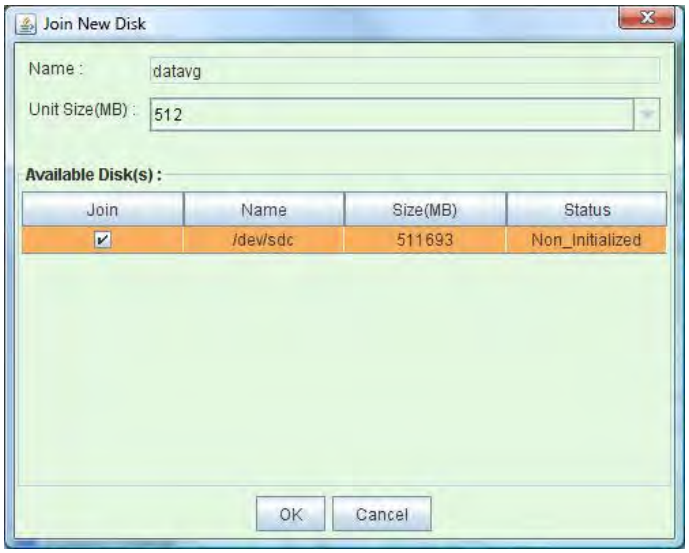
2. Enter the Volume Group Name. Click “Save” when done.



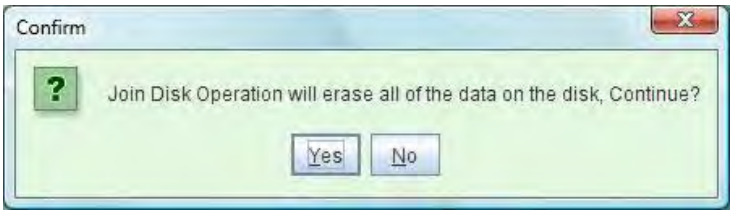
3. A confirmation message will appear. Select “Yes” to proceed.

4. Click “Join New Disk” to continue with creating the new Volume Group.

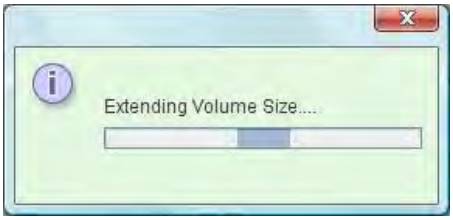
5. Check the disk(s) to be joined to the VG. Click “OK” when done.



6. A confirmation message will appear. Select “Yes” to proceed.



7. A process window will appear.



8. When the process of joining disk to the new VG is completed, the newly created VG will be shown.

NOTE: The new VG has no default Logical Volumes. Admin can create new Logical Volumes.

NOTE: The NAS supports up to 5 Volume Groups. Volume Group is the highest level of abstraction used within the NAS system. It gathers together a collection of Physical Volumes (consisting of at least one disk device, such as /dev/sdb) and Logical Volumes into one administrative unit.

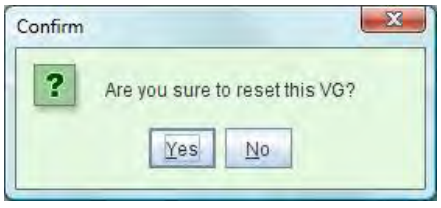
5.1.1.3 Reset and Remove Volume Group

NOTE: The system default Volume Group "proNASVG" cannot be deleted or reset.

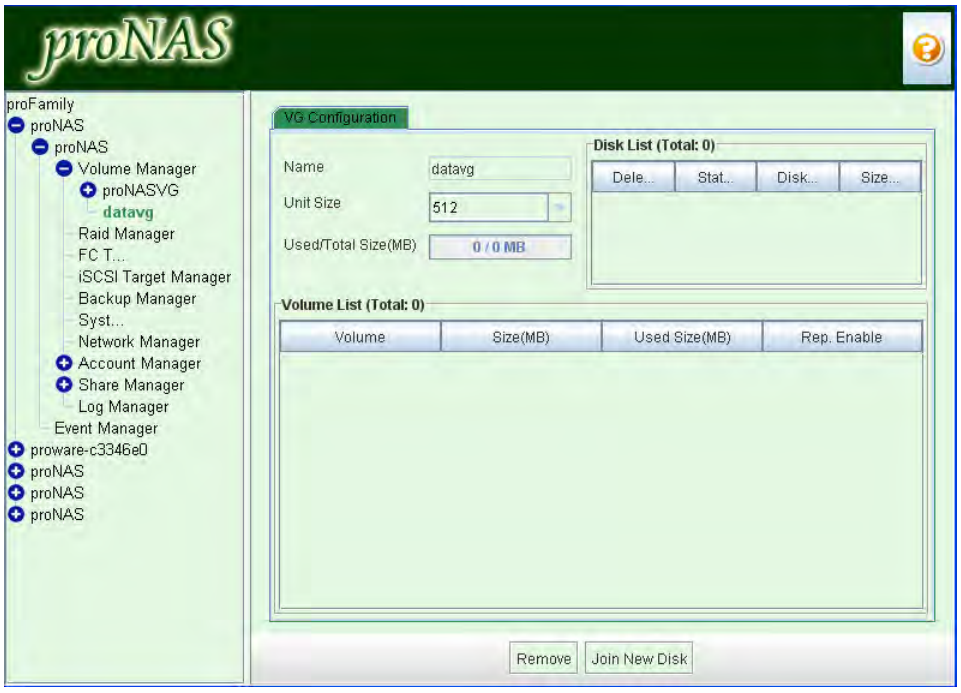
If you choose to reset a Volume Group, all the data will be erased. Use the "Reset Volume Group" function only when necessary, and when the data from the VG have been backed up or you do not want to keep the data.

1. Select the Volume Group name under Volume Manager, and click the "Reset Volume Group" button.

2. Select "Yes" to confirm.

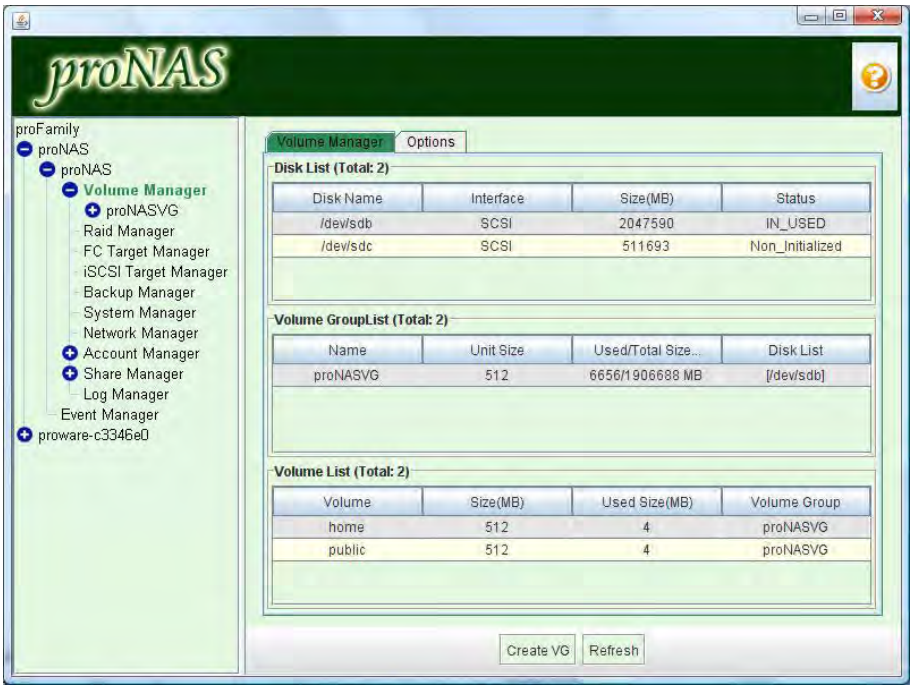


3. Click “Remove”.



4. Select “Yes” from the confirmation message.

5. Verify from Volume Group List in Volume Manager that the VG has been removed.

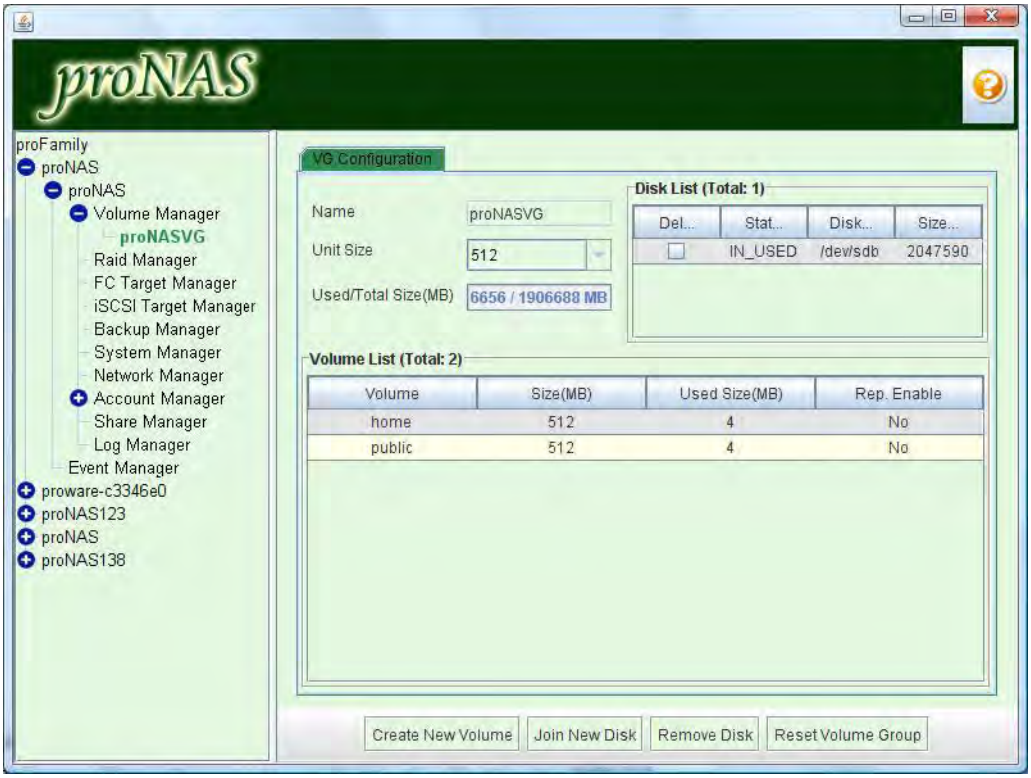


5.1.2 Logical Volume Configuration

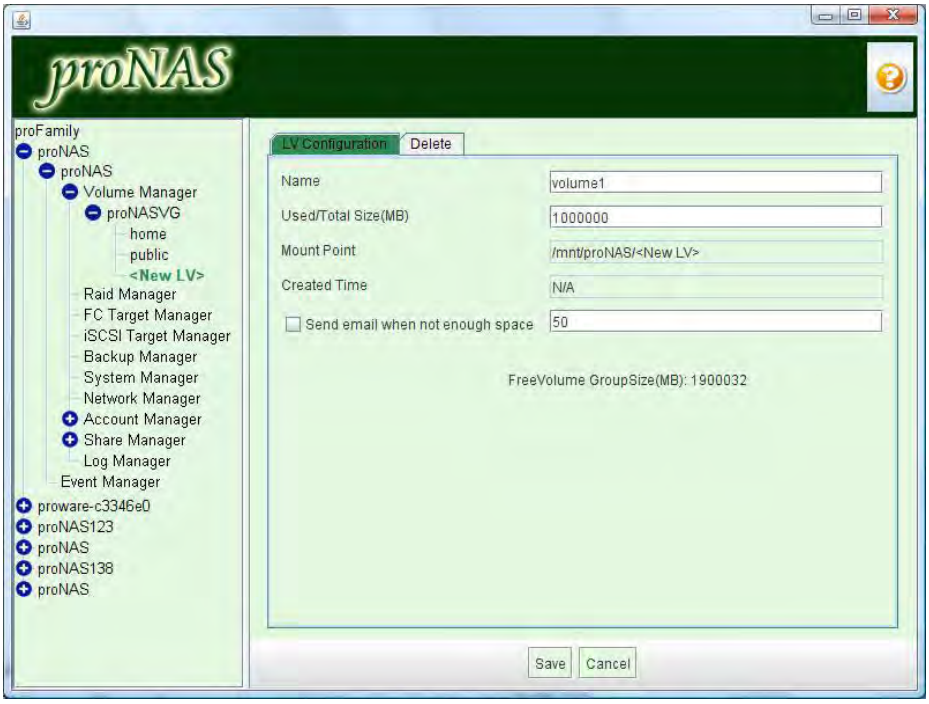
5.1.2.1 Create new Logical Volume

To create a new Logical Volume, follow these steps:

1. Double-click on a VG name. Click “Create New Volume” button.



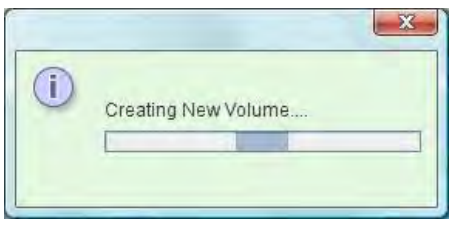
2. The LV Configuration tab will be displayed. Enter the Logical Volume name and the volume size (in MB). You can also enable the “Send email when not enough space” option to send an email notification to email recipients specified in Event Manager if the remaining free volume size is smaller than the size entered in this option. Click “Save” when done.



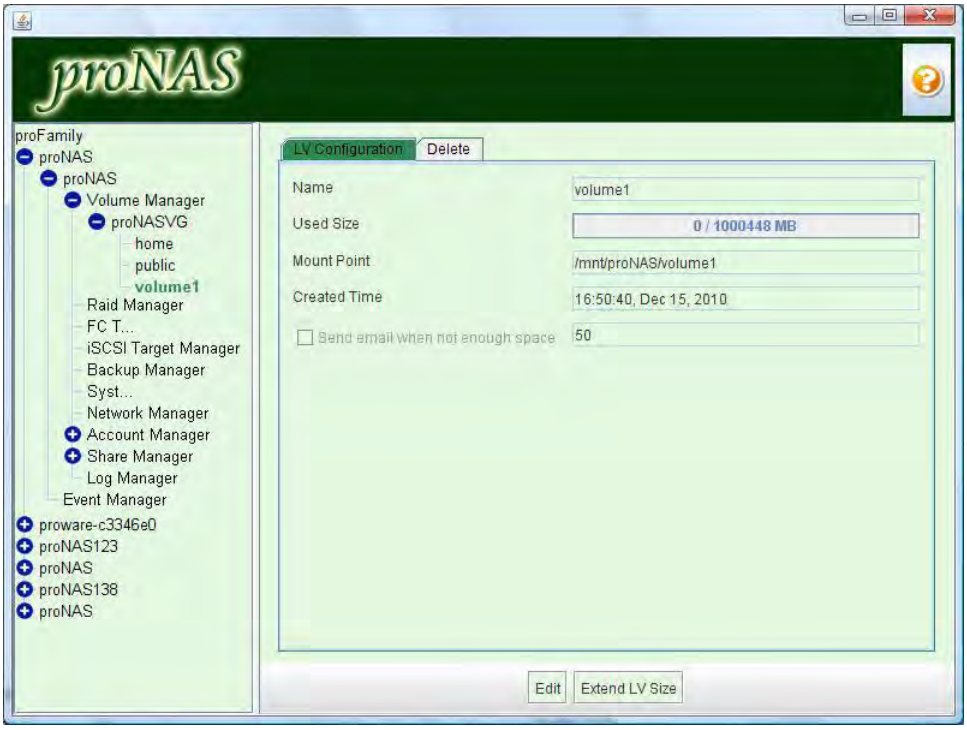
NOTE: The maximum LV size supported by proNAS version 1.3.xx is 8 exabytes (EB) or 8 billion gigabytes. If the LV will use Replication, the LV size can be set to 16TB (the maximum LV size supported by Replication function).

3. Select “Yes” from the confirmation message to create the LV.

4. A process window will be shown.



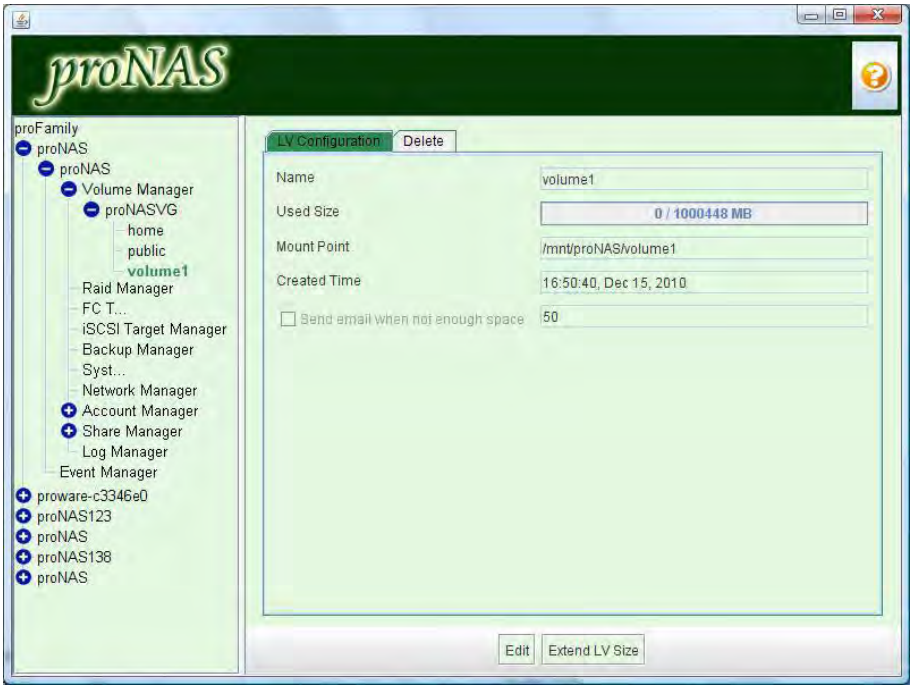
5. The new Logical Volume will be shown.



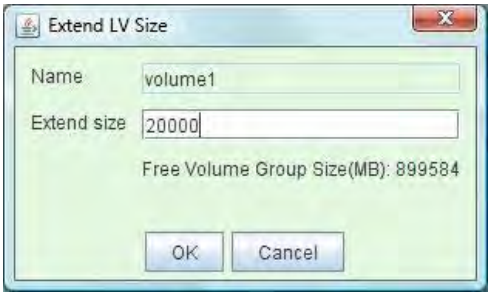
5.1.2.2 Extending Logical Volume Size

When the Logical Volume free space gets smaller and smaller, the Logical Volume size can be extended to allow more space for storing data. To extend the LV size, follow these steps:

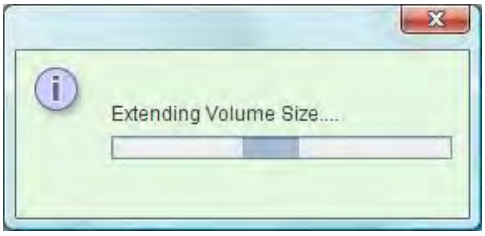
1. Select the LV that will be extended then click “Extend LV Size” button.



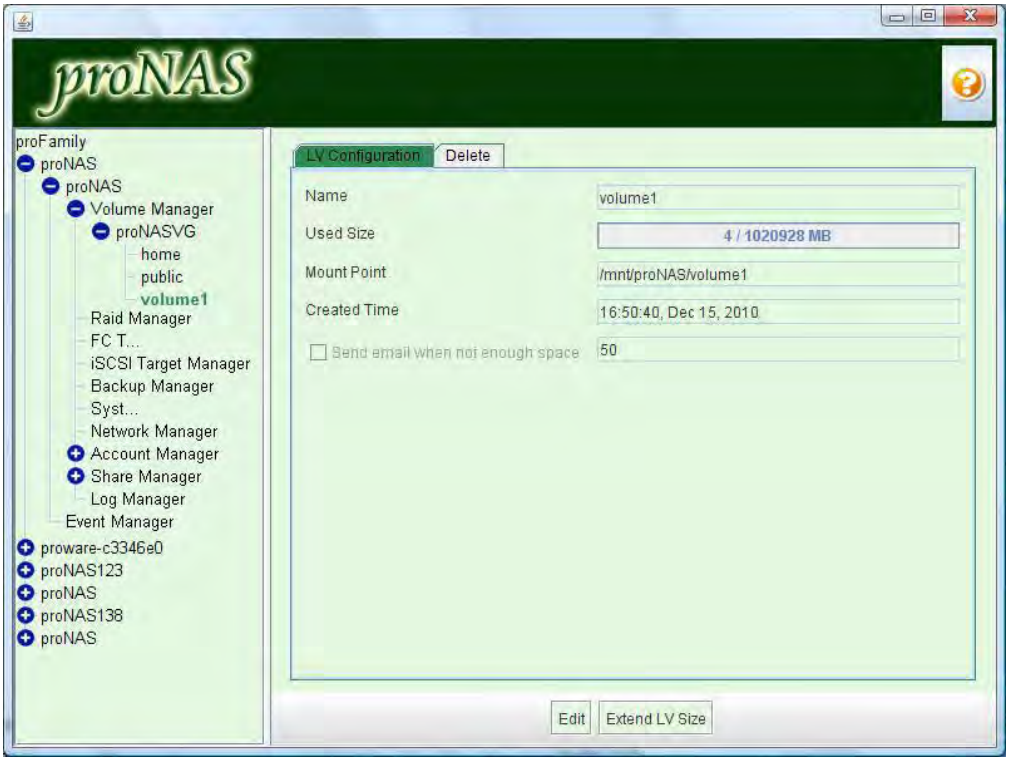
2. Enter in the “Extend size” box the additional size to be used for extension. Verify from the Free Volume Group Size (MB) the allowable size that can used in extension.



3. The Logical Volume will be extended.



4. Verify the new LV size.



5.1.3 Volume Snapshot

Snapshots are point-in-time copies of a logical volume. This allows the system administrator to create a new block device which presents an exact copy of a logical volume, frozen at some point in time. As changes are made to the original volume, the snapshot remains the same and looks exactly like the original at the time the snapshot was created.

A Snapshot can be created manually or scheduled. Admin need to enable first this special function.

NOTE: Logical Volume with snapshot cannot be extended nor replicated (see next section about Volume Replication).

To enable Snapshot function, select Volume Manager then click Options tab. Tick the “Enable Snapshot function” option.

NOTE: Creating Snapshots while a Logical Volume is under heavy I/O will slowdown the I/O access or interrupt the I/O process to a Logical Volume. This means that clients accessing the proNAS share, in which the Logical Volume is under snapshot, can experience slow write access.

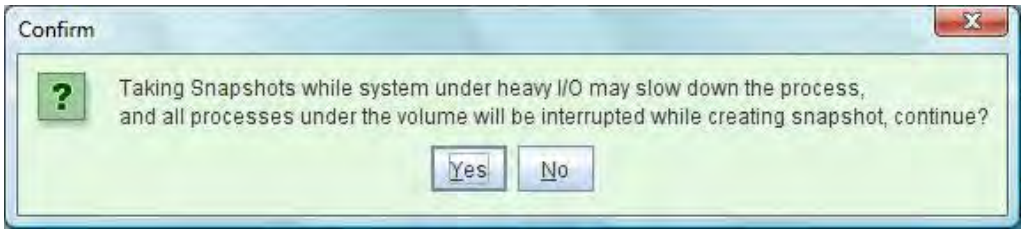
5.1.3.1 Create Snapshots in Logical Volumes

5.1.3.1.1 Create Snapshots Manually

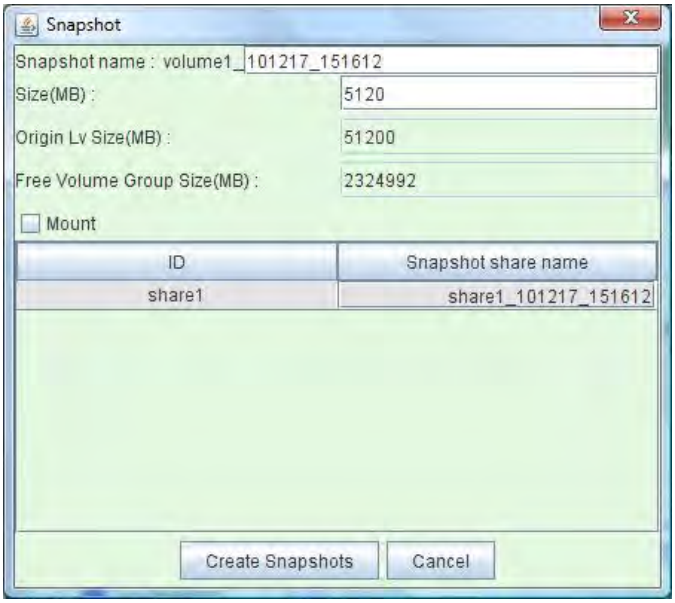
To manually create snapshots:

1. Select the Logical Volume, go to Snapshot tab and click “Create Snapshot”.

2. A confirmation message will appear. Select “Yes”.


Confirm
Taking Snapshots while system under heavy I/O may slow down the process,
and all processes under the volume will be interrupted while creating snapshot, continue?
Yes
No

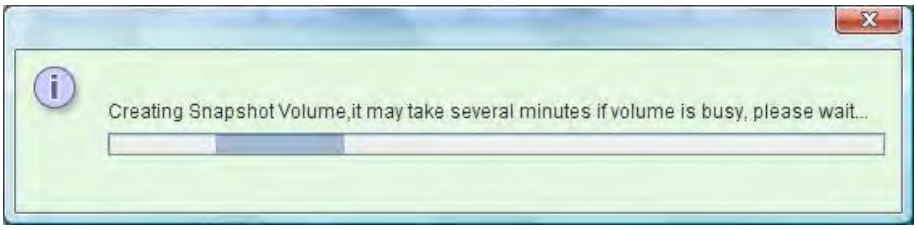
3. The Snapshot configuration window will be displayed. A system-created Snapshot name is automatically created. The default snapshot name can be renamed if needed. Enter the new Snapshot Size (in MB) if the size shown need to be changed. See details about Snapshot Options below. Click “Create Snapshots” to start creating snapshot.



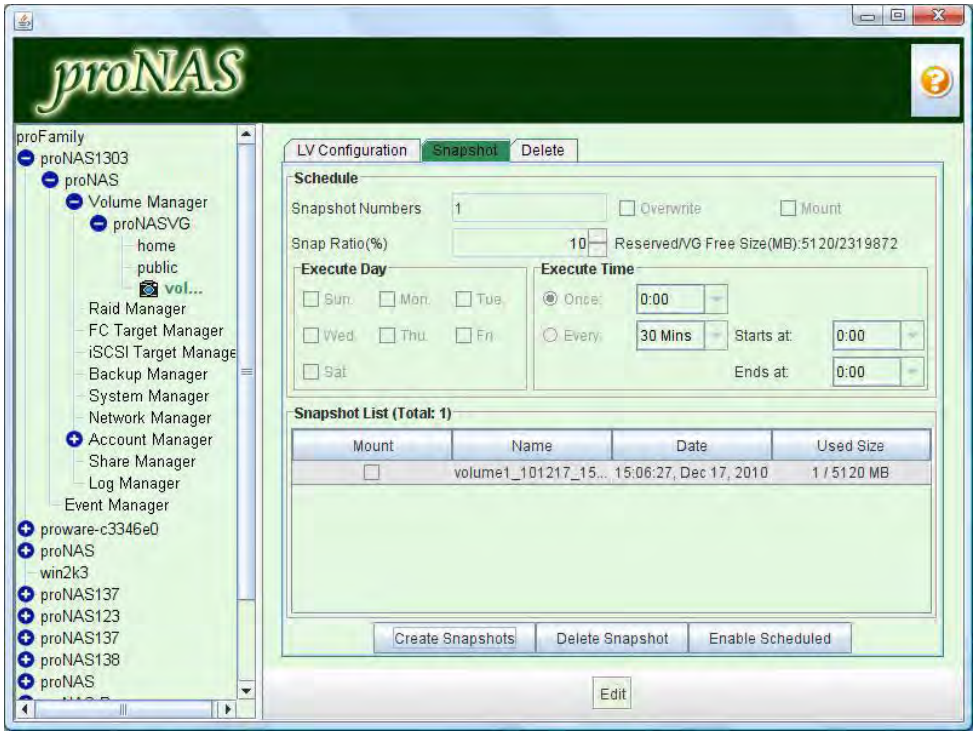
Snapshot Options:

- **Snapshot Name:** The default snapshot name is created by appending the date and time to the volume name. You can modify the snapshot name but the prefix volume name will still remain.
- **Size (MB):** This indicates the size of the snapshot volume that will be created. The default is 10% of the size of the logical volume where snapshot is to be taken. The size of the snapshot volume will be multiple of the PE size (VG Unit Size).
- **Origin LV Size:** This indicates the size of the Logical Volume where the new snapshot volume will be created.
- **Free Volume Group Size (MB):** This indicates the amount of free space on the volume group where the new snapshot volume will be created.
- **Mount:** When checked, the created snapshot volume will be automatically mounted. When a snapshot volume is mounted, the existing share from the snapshot volume will be accessible. Note that a snapshot volume is a read-only volume.
- **ID:** This specifies the shares created under this logical volume.
- **Snapshot share name:** This specifies the name of the snapshot shares. Your may access these shares by mounting the snapshot volume. The naming format used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "101217_151612".

4. A process window will be displayed.



5. When snapshot has been created, it will be shown in the Snapshot List of the Logical Volume.

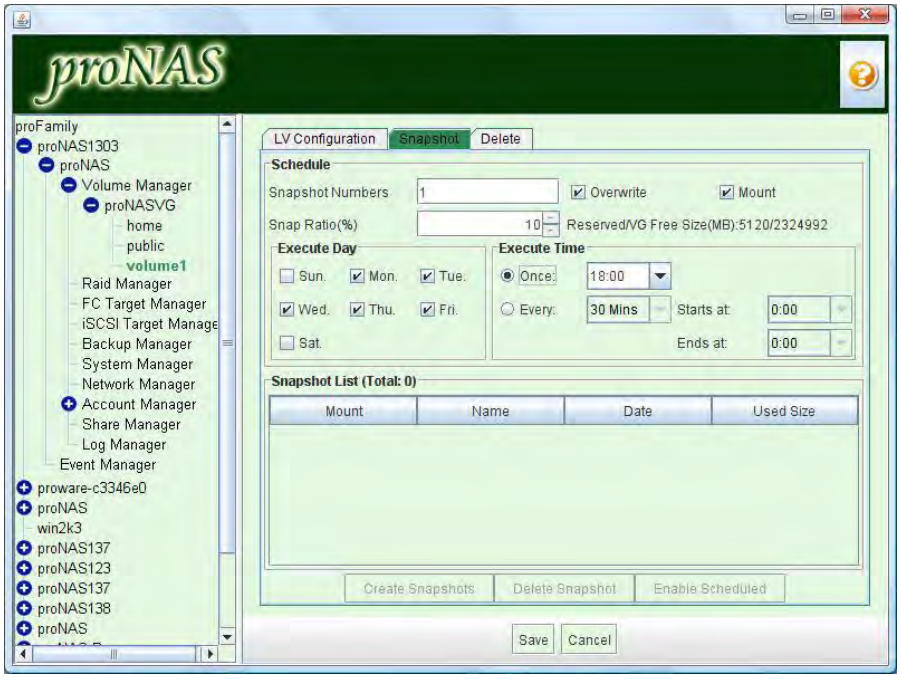


5.1.3.1.2 Create Snapshots Based from Schedule

To create scheduled snapshots:

1. Select the Logical Volume, go to Snapshot tab and click “Edit”.

2. Edit the Snapshot schedule options listed below then click “Save” when done.



Snapshot Options:

- **Snapshot Numbers:** Specifies the total number of snapshots that will be created.
- **Snap Ratio (%):** This is the ratio in percentage between the snapshot volume and the volume of origin. This indicates the ratio of the volume size that will be set as the size of the snapshot volume. For example, if your logical volume is 1GB and the Snap Ratio is 10%, the size of the snapshot volume that will be created is 512MB, assuming that your PE size (VG Unit Size) is 512MB. The snapshot volume size will always be a multiple of PE size and the smallest snapshot size is equal to the PE size.
- **Overwrite:** Selecting this option will automatically delete the oldest snapshot if the total number of snapshots is already exceeded.
- **Mount:** When checked, it means that the created scheduled snapshot will be automatically mounted.
- **Reserved/VG Free Size (MB):** The left side indicates the total volume space that will be used for the creation the snapshots. The right side indicates the free space of the volume group available for use.
- **Execute Day:** Specifies whether the scheduled task is to run on the selected day(s).
- **Execute time:**
  Once - Specifies the time of the day when the scheduled task will be taken.
  Every - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.
- **Snapshot Lists:**
  Mount - Allows you to mount the snapshot volume. All snapshot volumes will be mounted read-only. By mounting the snapshot volume, the files under this snapshot volume will become accessible.
  Name - This specifies the name of the snapshot volume. If the snapshots are created by schedule, proNAS will automatically create the snapshot name. The format that will be used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "101217_151612".
  Date - This indicates the date and time when the snapshot was created.
  Used Size - This indicates the space used by the snapshot data. The right side is the size of the snapshot volume. If the used space nearly exceeds the snapshot volume capacity, it will be set as "Invalid" and will be un-mounted automatically to keep the system consistent.

3. A confirm message window will be displayed. Select “Yes” to proceed.

4. An “Updating Volume Setting” message will be shown.

5. When the snapshot setting of LV has been set, click “Enable Scheduled” to active scheduled snapshot.

6. A clock-like icon will appear on the left side of the LV which means a scheduled snapshot is active. To disable the schedule, click “Disable Scheduled”.

7. After disabling the schedule, the “Enable Scheduled” button will become available.

5.1.3.2 Creating Snapshots in FC Target Manager

NOTE: FC Volume must be setup first in the FC Target Manager before configuring snapshots for the FC Volume.

NOTE: FC volume Snapshot does not support "overwrite" and "mount" functions in Snapshot tab in proNAS GUI.

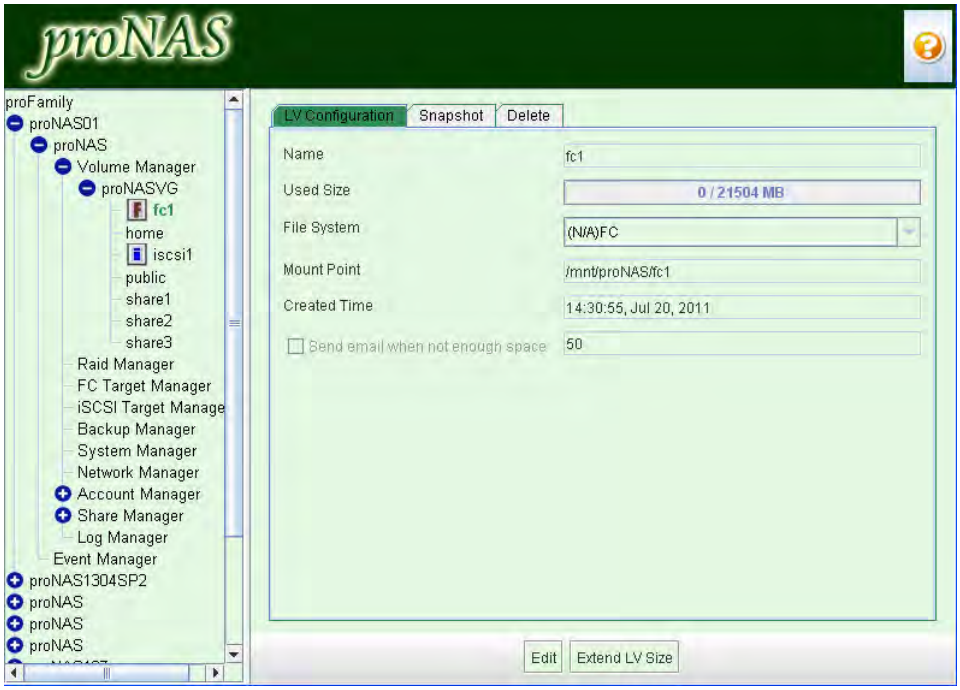
If Snapshot volume has exceeded the Snapshot reserved space, the Snapshot volume will become "Invalid". Please make sure you have enough reserved space for Snapshot.

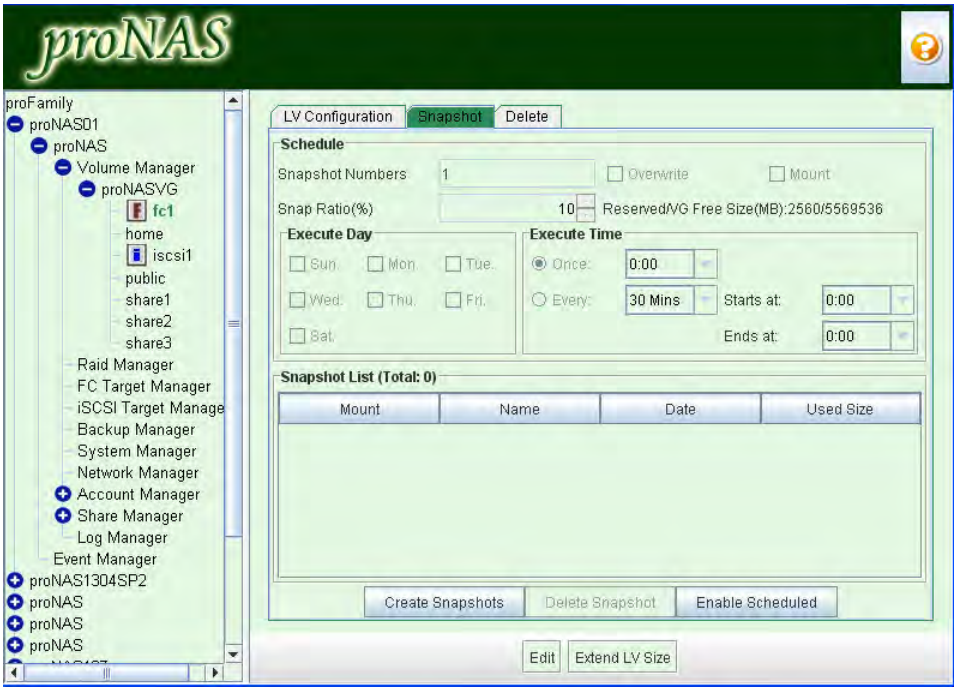
When you mount Snapshot volume for restoring data, please make sure there is no I/O access to the volume. If during this time, the Snapshot reserved space was exceeded and Shapshot volume became "Invalid", the host OS will not be able to access the Snapshot volume. The invalid Snaphot volume need to be deleted from Volume List, or host OS need to be restarted.

The "Snapshot Numbers" in Snapshot tab in proNAS GUI is for "rsh" Snapshot limit, and it is the number of Snaphots allowed when using "rsh".
The "Create Snapshots" button in GUI can also be used to manually create Shapshot for FC target volume or iSCSI target volume, and has no limit for Snapshot Numbers (can exceed the number of snapshots set in "Snapshot Numbers").

"rsh" command allows user to create Snapshot using other Linux OS that support "rsh".
How to use:
1. Enable "Telnet" serv ice in proNAS GUI.
2. In client Linux machine, execute rsh command
Syntax: rsh [IP address] –l [account] –n doSnapShot [proNAS LV name]

Where:
[IP address] = proNAS IP address, for example 192.168.100.150
[Account] = proNAS account, for example admin
[proNAS LV name] = proNAS LV name, for example iscsivol2
Example: rsh -l 192.168.100.150 -l admin -n doSnapshot iscsivol2


proNAS
proFamily
proNAS01
proNAS
Volume Manager
proNASVG
fc1
home
iscsi1
public
share1
share2
share3
Raid Manager
FC Target Manager
iSCSI Target Manage
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS1304SP2
proNAS
proNAS
proNAS
LV Configuration
Snapshot
Delete
Name
fc1
Used Size
0 / 21504 MB
File System
(N/A)FC
Mount Point
/mnt/proNAS/fc1
Created Time
14:30:55, Jul 20, 2011
Send email when not enough space
50
Edit
Extend LV Size


proNAS
proFamily
proNAS01
proNAS
Volume Manager
proNASVG
fc1
home
iscsi1
public
share1
share2
share3
Raid Manager
FC Target Manager
iSCSI Target Manage
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS1304SP2
proNAS
proNAS
proNAS
LV Configuration
Snapshot
Delete
Schedule
Snapshot Numbers
1
Overwrite
Mount
Snap Ratio(%)
10
Reserved/VG Free Size(MB):2560/5569536
Execute Day
Sun.
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Execute Time
Once:
0:00
Every:
30 Mins
Starts at:
0:00
Ends at:
0:00
Snapshot List (Total: 0)
Mount
Name
Date
Used Size
Create Snapshots
Delete Snapshot
Enable Scheduled
Edit
Extend LV Size

5.1.3.3 Creating Snapshots in iSCSI Target Manager

NOTE: iSCSI Volume must be setup first in the iSCSI Target Manager before configuring snapshots for the iSCSI Volume.

NOTE: iSCSI volume Snapshot does not support "overwrite" and "mount" functions in Snapshot tab in proNAS GUI.

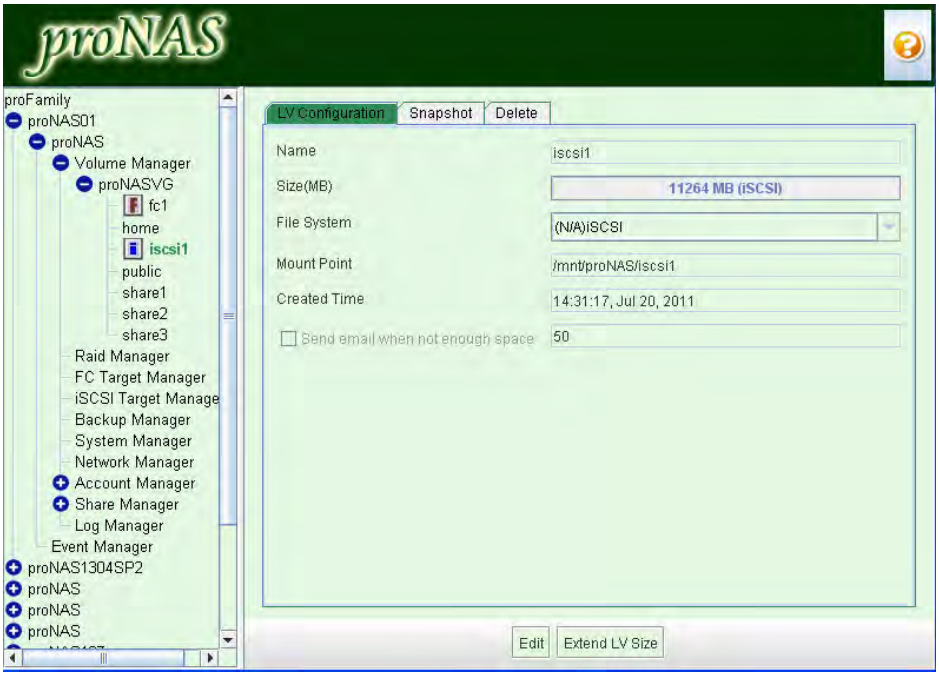
If Snapshot volume has exceeded the Snapshot reserved space, the Snapshot volume will become "Invalid". Please make sure you have enough reserved space for Snapshot.

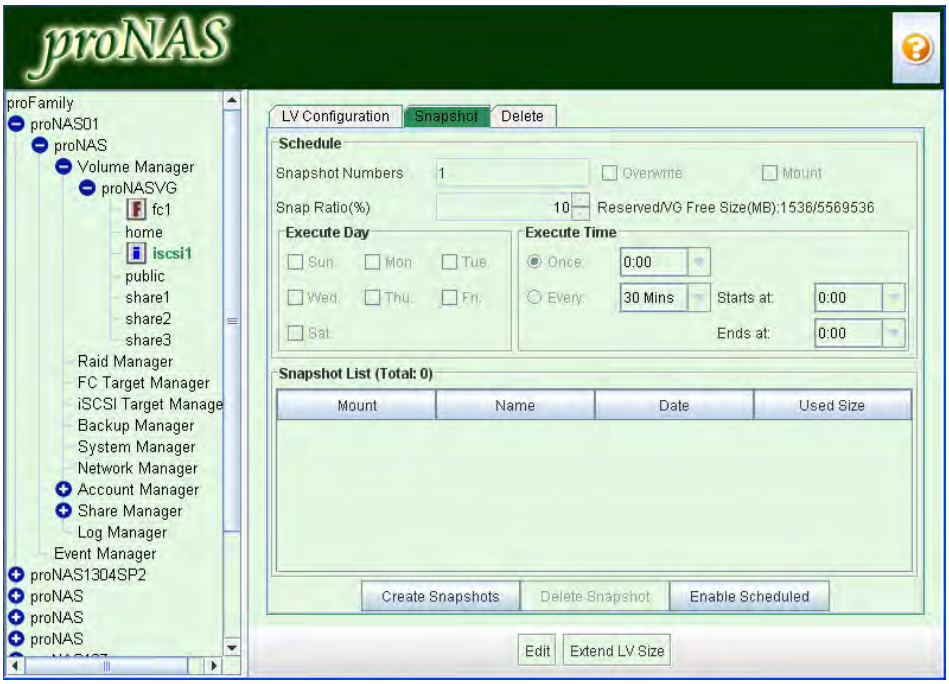
When you mount Snapshot volume for restoring data, please make sure there is no I/O access to the volume. If during this time, the Snapshot reserved space was exceeded and Shapshot volume became "Invalid", the host OS will not be able to access the Snapshot volume. The invalid Snaphot volume need to be deleted from Volume List, or host OS need to be restarted.

The "Snapshot Numbers" in Snapshot tab in proNAS GUI is for "rsh" Snapshot limit, and it is the number of Snaphots allowed when using "rsh".
The "Create Snapshots" button in GUI can also be used to manually create Shapshot for FC target volume or iSCSI target volume, and has no limit for Snapshot Numbers (can exceed the number of snapshots set in "Snapshot Numbers").

"rsh" command allows user to create Snapshot using other Linux OS that support "rsh".
How to use:
1. Enable "Telnet" serv ice in proNAS GUI.
2. In client Linux machine, execute rsh command
Syntax: rsh [IP address] –l [account] –n doSnapShot [proNAS LV name]

Where:
[IP address] = proNAS IP address, for example 192.168.100.150
[Account] = proNAS account, for example admin
[proNAS LV name] = proNAS LV name, for example iscsivol2
Example: rsh -l 192.168.100.150 -l admin -n doSnapshot iscsivol2

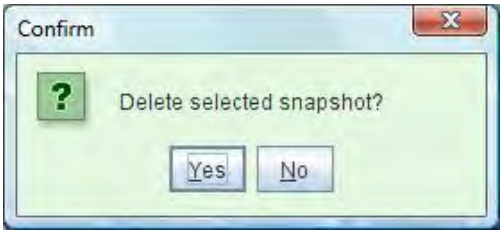

proNAS
proFamily
proNAS01
proNAS
Volume Manager
proNASVG
fc1
home
iscsi1
public
share1
share2
share3
Raid Manager
FC Target Manager
iSCSI Target Manage
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS1304SP2
proNAS
proNAS
proNAS
LV Configuration
Snapshot
Delete
Name
iscsi1
Size(MB)
11264 MB (iSCSI)
File System
(N/A)iSCSI
Mount Point
/mnt/proNAS/iscsi1
Created Time
14:31:17, Jul 20, 2011
Send email when not enough space
50
Edit
Extend LV Size


proNAS
proFamily
proNAS01
proNAS
Volume Manager
proNASVG
fc1
home
iscsi1
public
share1
share2
share3
Raid Manager
FC Target Manager
iSCSI Target Manage
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
Event Manager
proNAS1304SP2
proNAS
proNAS
proNAS
LV Configuration
Snapshot
Delete
Schedule
Snapshot Numbers
1
Overwrite
Mount
Snap Ratio(%)
10
Reserved/VG Free Size(MB):1536/5569536
Execute Day
Sun.
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Execute Time
Once
0:00
Every
30 Mins
Starts at:
0:00
Ends at:
0:00
Snapshot List (Total: 0)
Mount
Name
Date
Used Size
Create Snapshots
Delete Snapshot
Enable Scheduled
Edit
Extend LV Size

5.1.3.4 Delete Snapshots

1. Select the Logical Volume where snapshot will be deleted, then go to Snapshot tab. Click the snapshot that will be deleted then click “Delete Snapshot”.

2. Select “Yes” to delete the snapshot.



3. A process window will be shown.

4. The deleted snapshot will no longer exist in the Snapshot List.

5.1.4 Volume Replication

Replication function enables proNAS to replicate a logical volume from one NAS server (source) to another NAS server (destination). Replication involves intelligent copying and maintaining of exact copy of a volume from a source server to a destination server. The destination volume is always an exact copy of the source volume. This is done by mirroring the whole block device via a standard network interface. This solution creates a real time replication of data. However, it does not create a cluster solution where you can have a highly available system.

Note: Logical Volume under Snapshot cannot be replicated.

NOTE: In proNAS version 1.3.xx, Replication of Logical Volumes with LV capacity up to 16TB is supported.

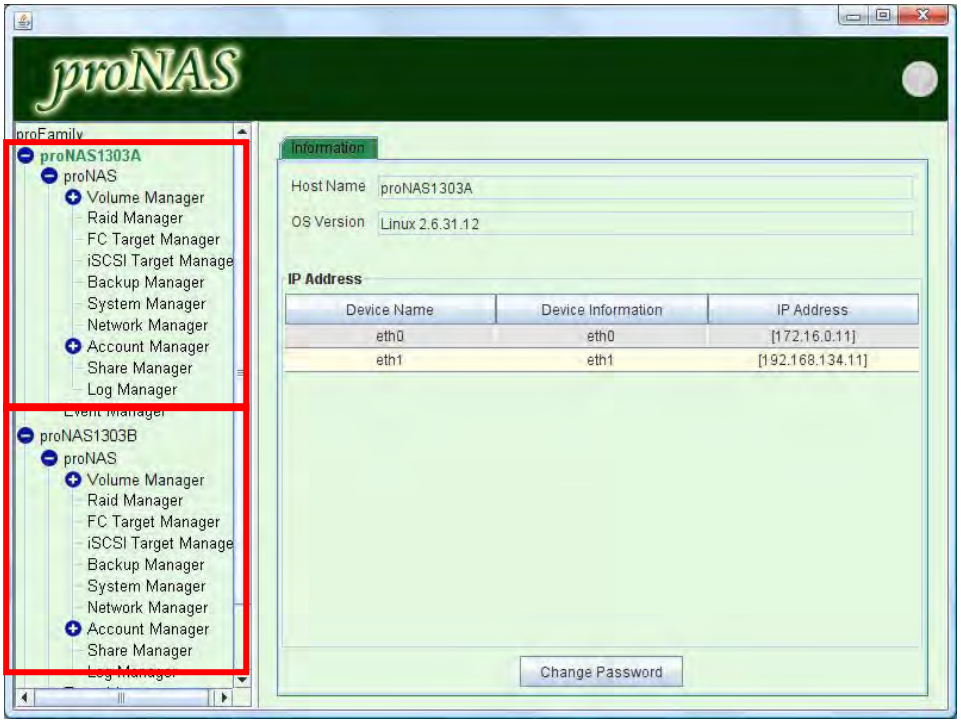
To enable Replication, select Volume Manager then click Options tab and tick “Enable Replication function”.

NOTE: Make sure the two proNAS servers have different host names before setting up Replication.
It is advisable to configure a network port, in each of the two NAS servers, as dedicated channel/medium for Replication.

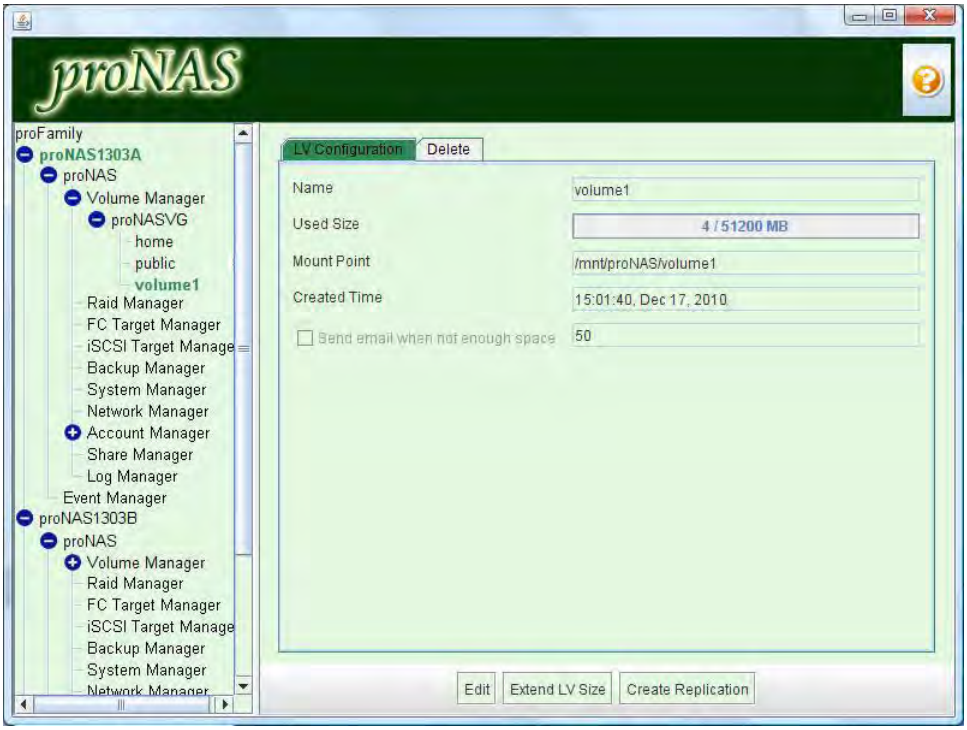
5.1.4.1 Replication Configuration

To setup Replication between two NAS servers:

1. Admin need to login to the proNAS management GUI of the two NAS servers.



2. On the primary NAS (source), select the Logical Volume which will be replicated, then click “Create Replication”.



NOTE: The logical volume to be replicated from source proNAS must not exist in the destination proNAS. If the destination proNAS has the same logical volume, Replication cannot be setup.

3. The Create Replication window will be displayed. Set the options below and click "OK" when done.

Replication Options:

[Remote]

- **Local** - Select the IP address of the local (source) proNAS that will be used for replication.
- **Remote** - Select or type manually the IP address of remote (destination) proNAS that will be used for replication.

NOTE: The local and remote IP addresses serve as the channel between the source and destination NAS servers. This is where the replication of data takes place. Please be sure to have a good connection on this medium. As much as possible, set this channel as a dedicated or a private network. It is recommended to use different Ethernet port for replication from the Ethernet port used for data access. It is best to use a crossover network link between the Ethernet ports involved. Refer to Network Manager Section for configuring Ethernet port.

- **Remote VG** - Select the VG on remote proNAS where the replicated logical volume will be created.

[Setting]

- **Port to Bind** - A TCP port to bind locally and is used to connect to the remote node. Default is 7788.

NOTE: User cannot use ports that already have been used. Available ports are from 7788 to 77xx.

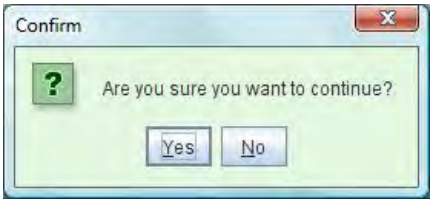
- **Connection Type:** proNAS supports two types of data replication protocols:
  - **Sync** - Synchronous. The system will acknowledge the transaction as completed after the data is written to the disk of destination proNAS. It is recommended to use this mode. In most cases, this connection type preserves transaction semantics. Write IO is reported as completed if it has reached the remote disk.
  - **Async** (for high latency network) - Asynchronous. The system will acknowledge the transaction as completed after the data is written to buffer. It provides faster transmission and is suitable for busy network. Write IO is reported as completed if it has reached the local TCP send buffer.
- **Max Sync Rate** – This sets the limit of the bandwidth that will be used by the synchronization process. Default is 30MB/sec. Minimum value is 4MB/sec and maximum value is 680 MB/sec – for high latency network environment (e.g. bonding on Gigabit Ethernet).
- **Send buffer size (K)** - It is the size of the TCP socket send buffer. You can specify smaller or larger values. Larger values are appropriate for reasonable write throughput with asynchronous protocol over high latency networks. Default is 512K and maximum is 1024K.
- **Time out (sec)** - It is the value to wait for connection timeout if the remote node is degraded. If the remote node fails to send the response packet within the specified timeout time, the remote node will be considered dead and the TCP/IP connection is abandoned. The default is 6 sec. Minimum is 1 sec and maximum is 60 sec.

- **When Lost Connection**: When the replication connection is lost, the replication program can either go stand-alone or will try to reconnect.

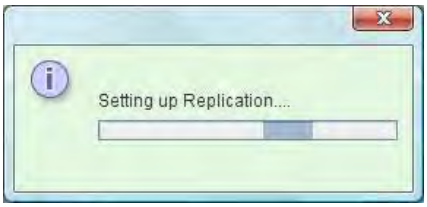
  - **Reconnect:** The replication program will attempt to reconnect. (Default)
  - **Stand-alone:** The replication program will not attempt to reconnect and will go on stand-alone state. All IO request are only passed locally and no replication.

NOTE: Before replication will be successfully created, a 4GB logical volume will be created on each node. This will serve as the metadata device for the replicated volume. This volume is not mounted and will not be seen on the proNAS GUI. Please be sure to have an extra 4GB space on either side of your NAS nodes.

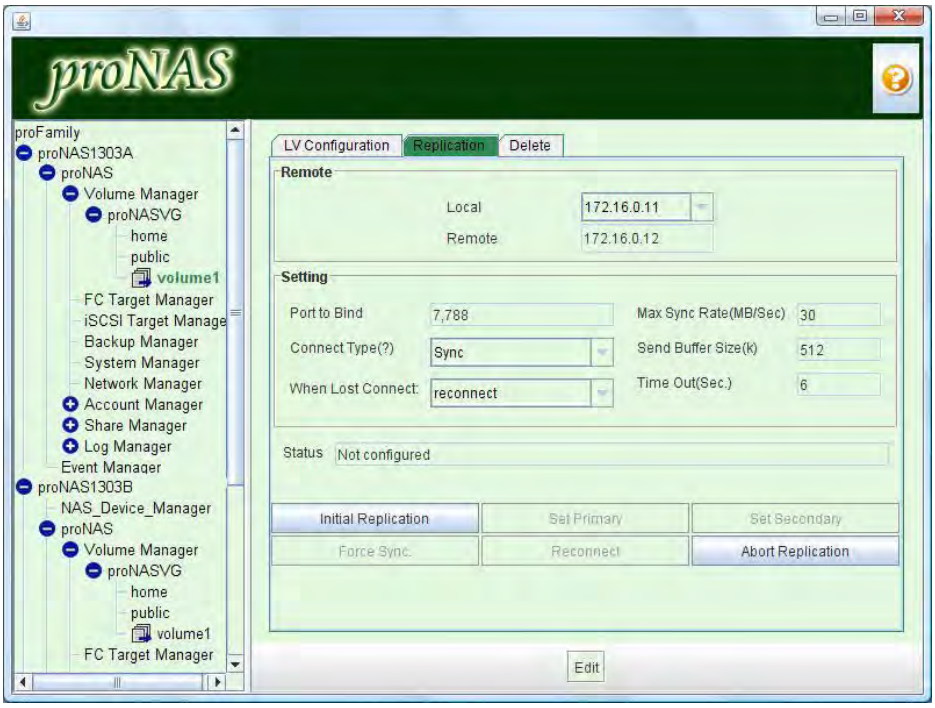
4. A confirmation message will be displayed. Click “Yes” to continue.



5. A message box will be displayed. When completed, Replication is enabled in the LV.

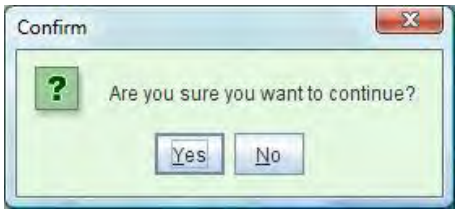


6. Select the LV name, then click Replication tab. Initialize the Replication by clicking “Initial Replication” button. When the confirmation message is displayed, select “Yes” to continue.

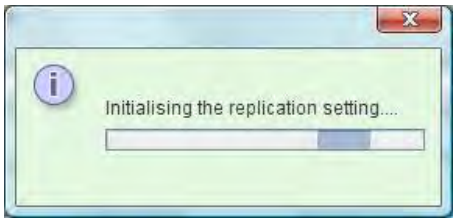


NOTE: After creating Replication on a logical volume, a similar logical volume will be created on the destination server under the specified VG. At this point, the Replication is not yet initialized and no synchronization. Replication still needs to be initialized. After selecting “Initial Replication” button, the first node will then connect to the second node and starts to synchronize. Synchronization typically takes quite a while especially on larger logical volumes. After initializing, the source node should be in "Primary" state and the destination node should be in "Secondary" state. If this is the state, you have now a working replication. Initializing should be done in the source volume.

7. In the Confirm message, select “Yes” to continue.



8. The volume replication setting will be initialized.



9. The volume replication synchronization process will start.

NOTE: The time it takes to completely initialize (sync) the source volume and destination volume depends on the size of the source volume. Larger volume takes longer time. The percent completed, estimated time to finish, and the replication sync speed is shown in Status information.

10. After the initial synchronization process is completed, the Status will show “Primary/Secondary, UpToDate/UpToDate”.

5.1.4.2 Checking the Status of Replication

Primary: The node of source volume. All the writing and reading are done on the primary node.

Secondary: The node of destination volume. The replicated data on the secondary node is used for backup only and is not accessible. Only the source data is accessible during replication.

Unknown: The node fails to establish connection.

UpToDate: The node is updated.

Setting the replicated volume on destination proNAS to be Primary

To set the replicated volume to primary, first you need to set both nodes to Secondary. This can be done by setting the primary to be secondary. After both nodes becomes Secondary/Secondary, go to the management GUI of the destination node. Under the replicated logical volume, click the "Set Primary" button.

WARNING! The replicated volume on the Secondary node must not be mounted. Please do not attempt to mount it manually.

Setting the primary volume to be secondary

To set the primary volume to be secondary, just press the "Set Secondary" button on the primary node.

Forcing the synchronization

To manually force the synchronization, press the "Force Sync." button. The data on the primary node will be forcefully synchronized to the secondary node.

Reconnect when the connection of the peer is lost.

To reconnect the replicated volume, press the "Reconnect" button. At some point if the replication fails to establish connection to the other node, you may try to set up a connection thru this button. This button will be enabled only if one of the node losses connection.

Aborting the Replication

To abort or drop the Replication, press the "Abort Replication" button. After aborting the Replication, the data on the destination volume can be retrieved by accessing the share folder under that destination volume, and the share folder name is exactly the same as the share folder on the source volume.

5.1.4.3 Extending Logical Volume under Replication

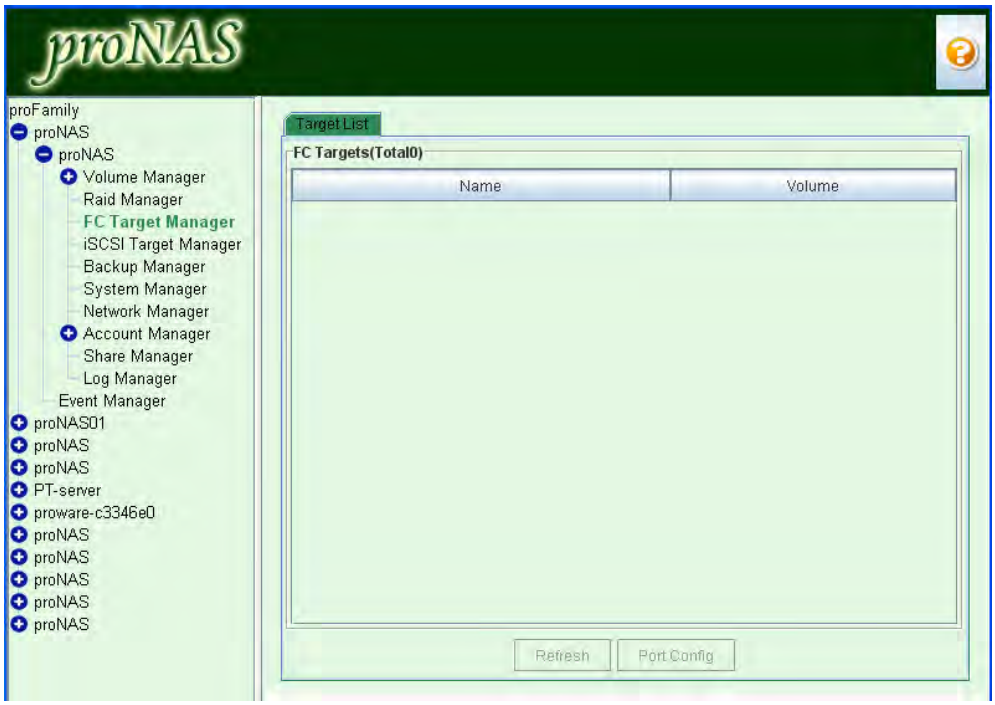
NOTE: Extending the size of a Logical Volume under Replication is not allowed. However, there is a work around to extend the LV size. Note that the extended LV size must not exceed 16TB.

The following are the steps:

1. Abort the replication by selecting “Abort Replication”.
2. Remove or delete the replicated logical volume on the destination proNAS.
3. Extend the capacity of the source logical volume. Please note that there should be enough space on the VG of the destination proNAS to accommodate the extended logical volume space.
4. Create a new Replication using the extended source logical volume.

5.2 FC Target Manager

The FC Target Manager allows configuration of Volumes as FC target LUNs.



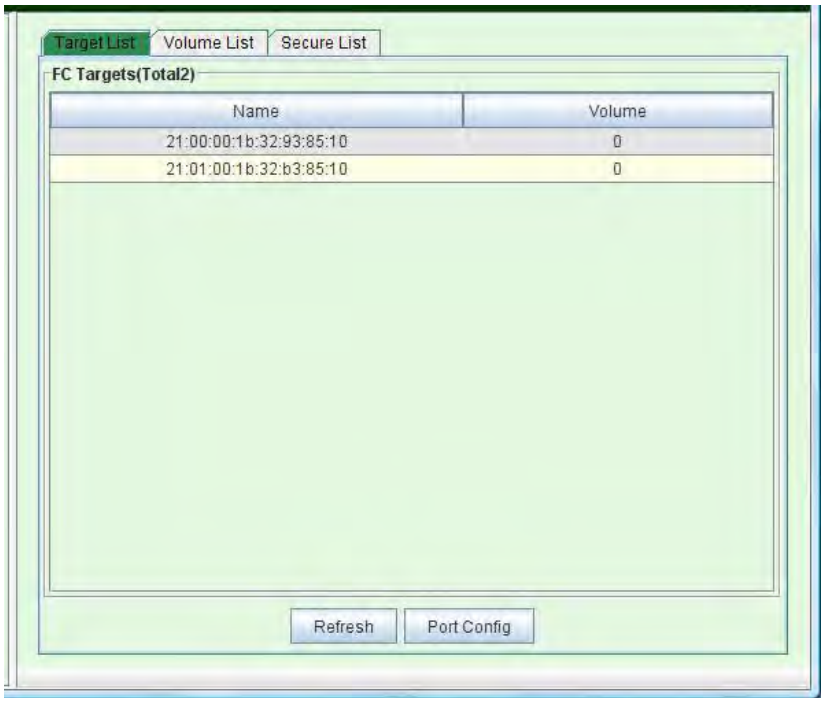
NOTE: FC target supports only QLogic FC HBA, such as QLE246x 4Gb and QLE256x 8Gb adapters.

NOTE: The following are the FC Target Limitations:

- ☑ **Only one client can access one FC target**
- ☑ **FC target maximum LUN mapping is up to 64**
- ☑ **The maximum FC target depends on number of FC port on FC HBA; for example, if there are 2 FC ports, then the maximum FC target is 2 (as shown in Target List)**

5.2.1 Target List

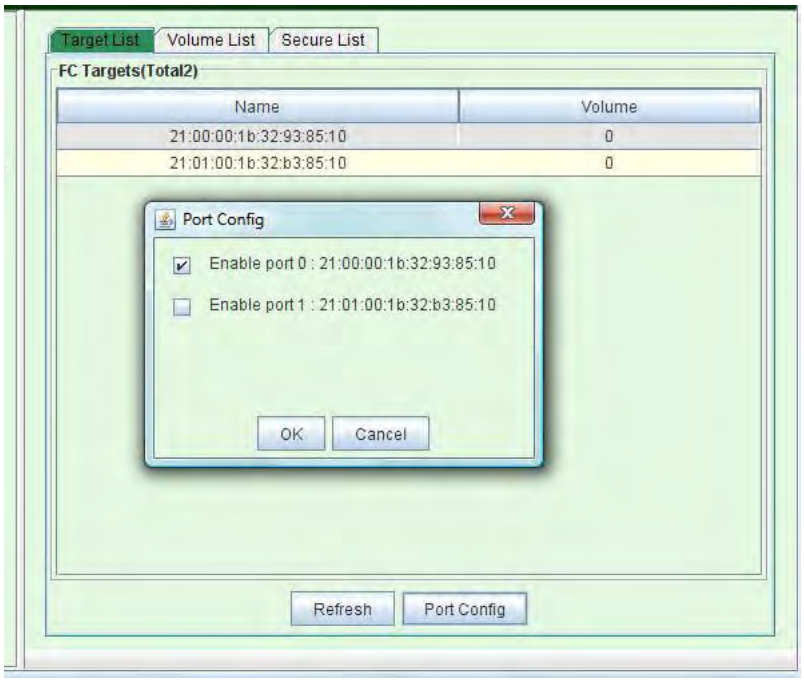
Using the Target List, the FC Target Name can be configured. This also shows the list of FC target names.



5.2.1.1 Port Config

The FC port(s) on the NAS must be configured/enabled first in Target List.

1. To configure FC port, click “Port Config”.

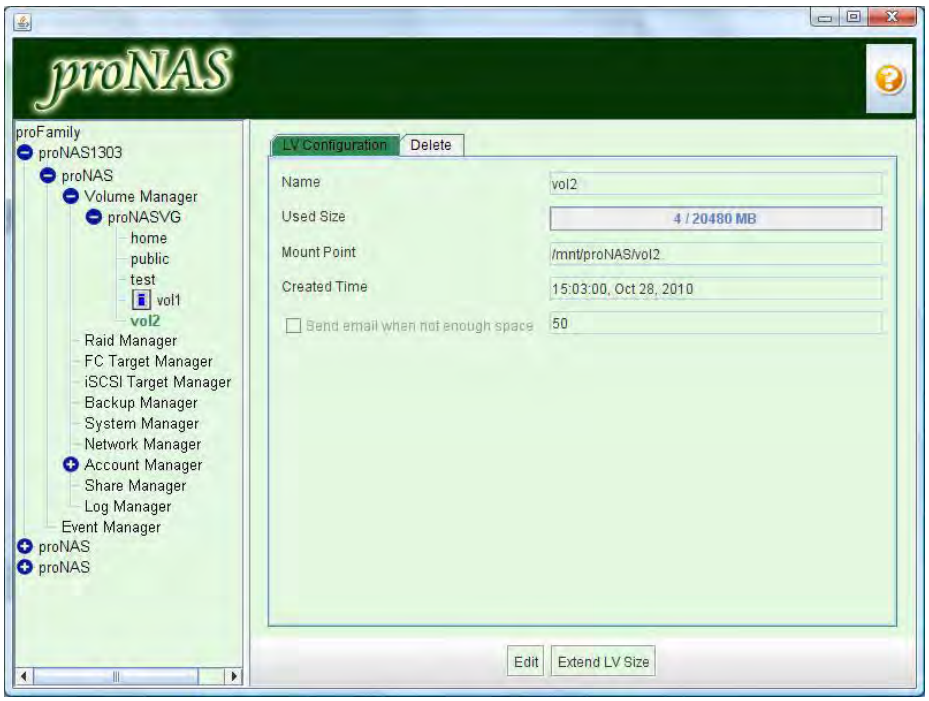


2. Enable which FC port on the FC HBA on NAS will be used or connected to FC switch or FC HBA on host side. Select “Enable port0” or “Enable port1”. Click “OK” when done.

5.2.2 Volume List

The Volume List is used to create, edit, or delete FC Target Volumes. This also shows the list of FC target volumes.

NOTE: A Volume that will be used as FC Target Volume must be created first in Volume Manager under a Volume Group (proNASVG, in this example), if one is not yet created.



A Volume “vol2” created for FC target volume use

To create a FC Target Volume:

1. Select Volume List, and then click “Create”. In the Volume List, select the Target Name (FC WWN), and then select the volume name previously created and reserved as FC target volume, in this example “vol2” is selected.

   Note that the LUN ID and Block Size settings will normally work and need not be changed.

2. Click “OK” when done. The volume will be shown in the list.

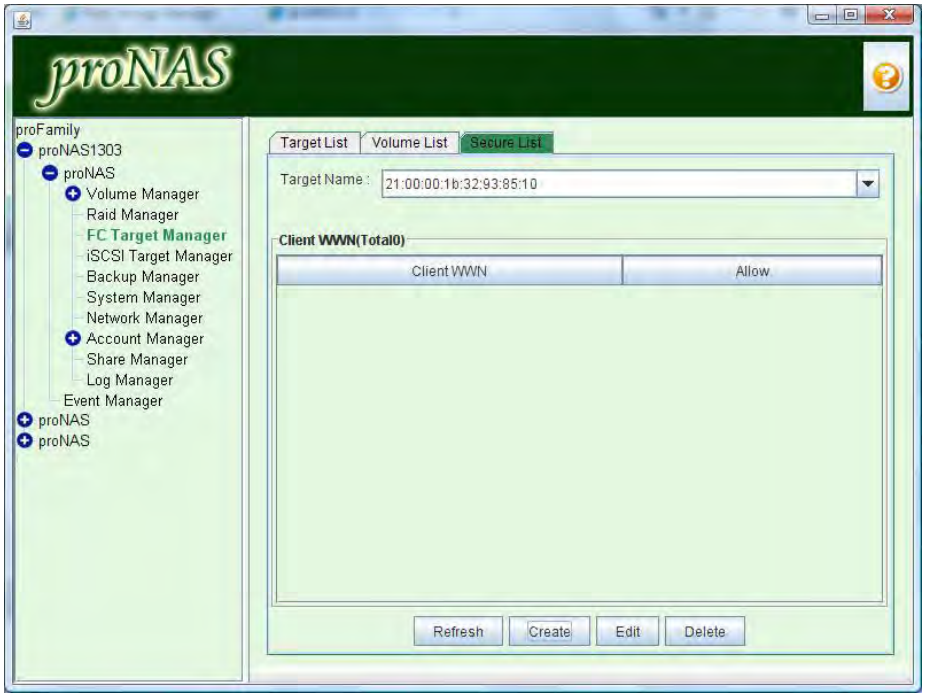
5.2.3 Secure List

The Secure List is used to configure FC target volumes Host Filter, to allow certain hosts from accessing the FC Target Volumes.

NOTE: By default, all clients are denied access to the FC target volume. Only one client can access one FC target.

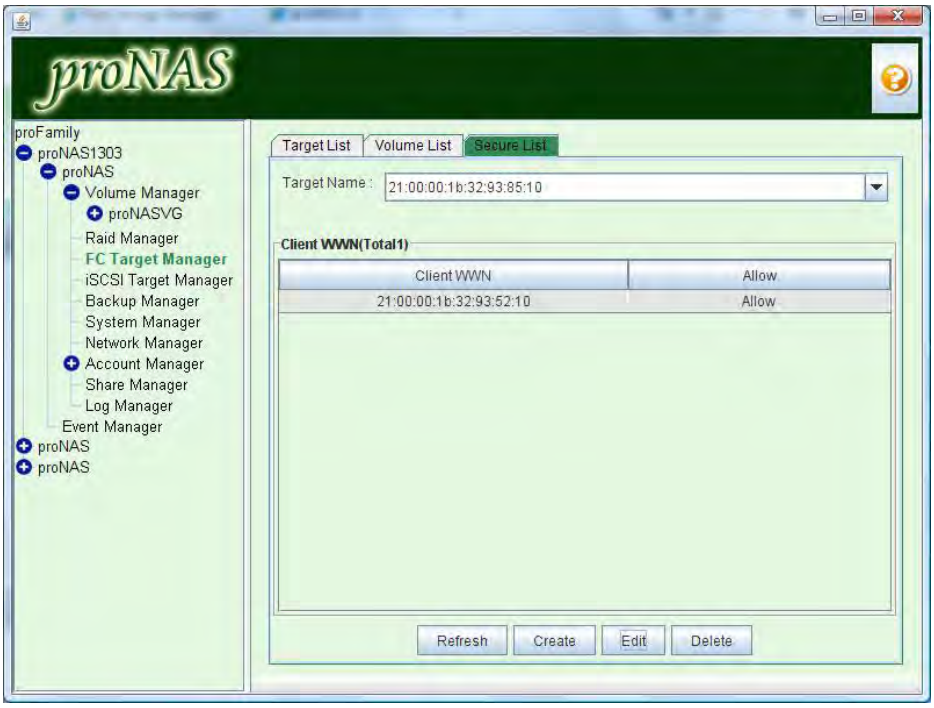
To configure Secure List:

1. Select “Secure List”. Click “Create” to add FC WWN that will be allowed access to the FC Target Volume.



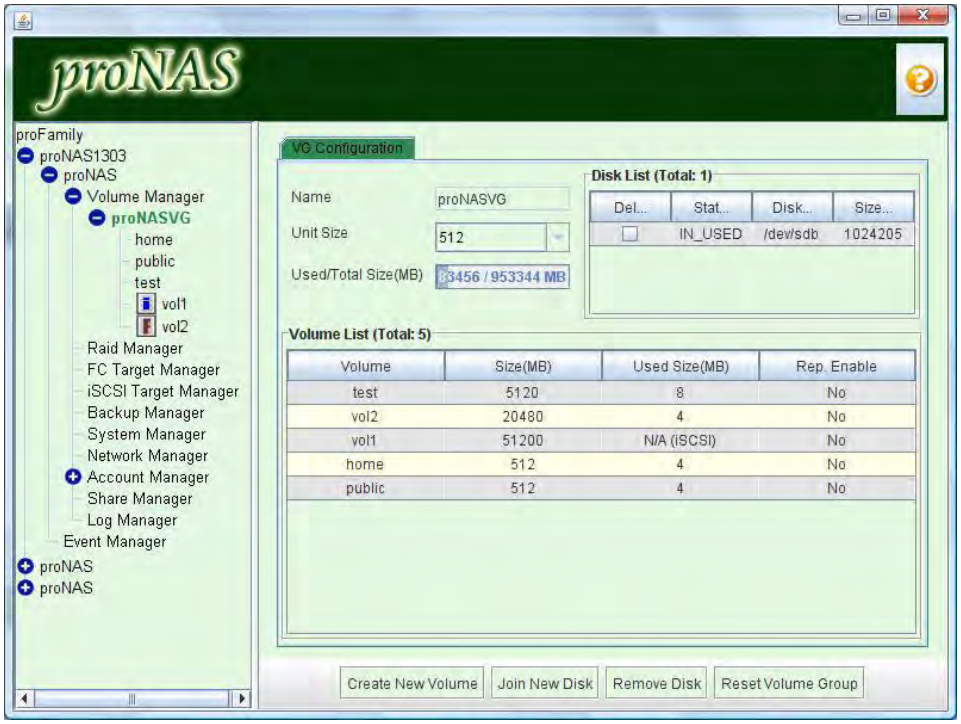
2. Enter the Client WWN that will be allowed access. The example used here is: 21:00:00:1b:32:93:52:10. Click “OK” when done.

3. The Client WWN is added to the Secure List and is allowed access to the specified Target Name.



NOTE: Only the FC WWN included in the list will be allowed access to the FC target volume (LUN). Other FC WWN clients not in the list will not see the LUN.

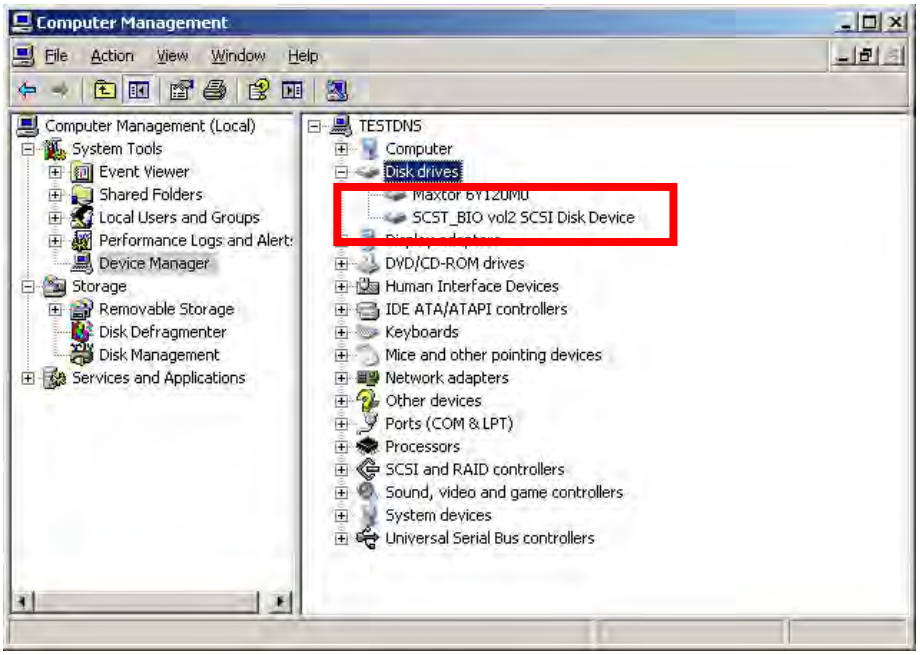
4. Click “Volume Manager” and the VG (proNASVG) where the volume was created. Note the FC Target Volume has an “**F**” icon.



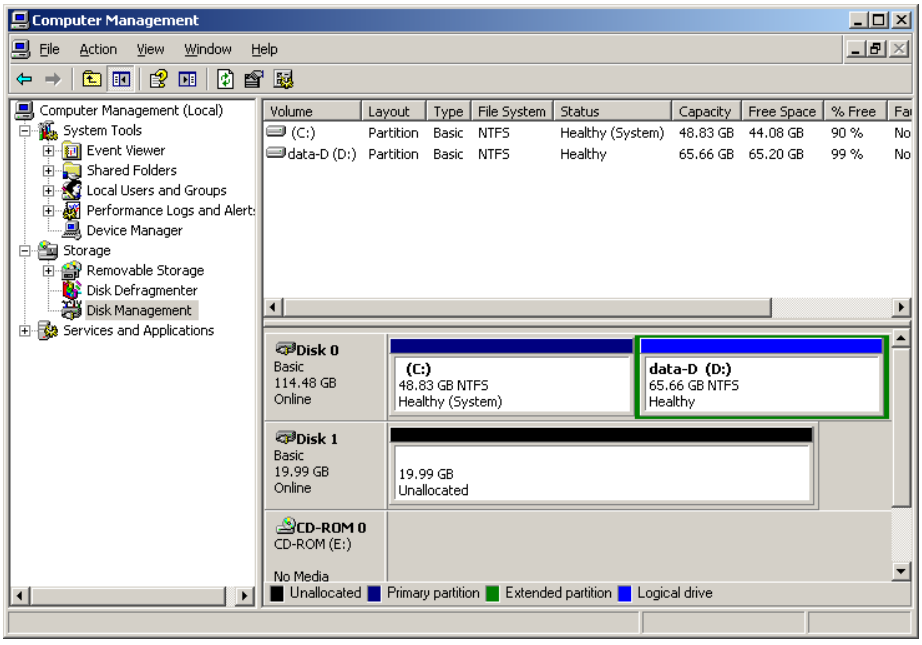
5.2.4 Connecting Host to FC Target Volume

To connect a host to FC target volume:

1. Connect the Host OS to the FC Target Volume. In this example, the Host OS is running Windows Server 2003 SP2 and the FC HBA WWN is 21:00:00:1b:32:93:52:10 (which is the “Client WWN” setup in Secure List). The FC Target Volume is shown in Device Manager – Disk Drives. Do “Rescan of device” if necessary.



2. In Disk Management, initialize and format the Disk device.



5.3 iSCSI Target Manager

The iSCSI function in proNAS makes a logical volume become an iSCSI target LUN.

NOTE: The following are the iSCSI Target Limitations:

- ☑ **Only one initiator (client IP) can access one iSCSI target volume**
- ☑ **iSCSI target maximum LUN mapping is up to 64**

5.3.1 Target List

From the Target List window, an iSCSI target name can be configured. This also shows the list of iSCSI target names.

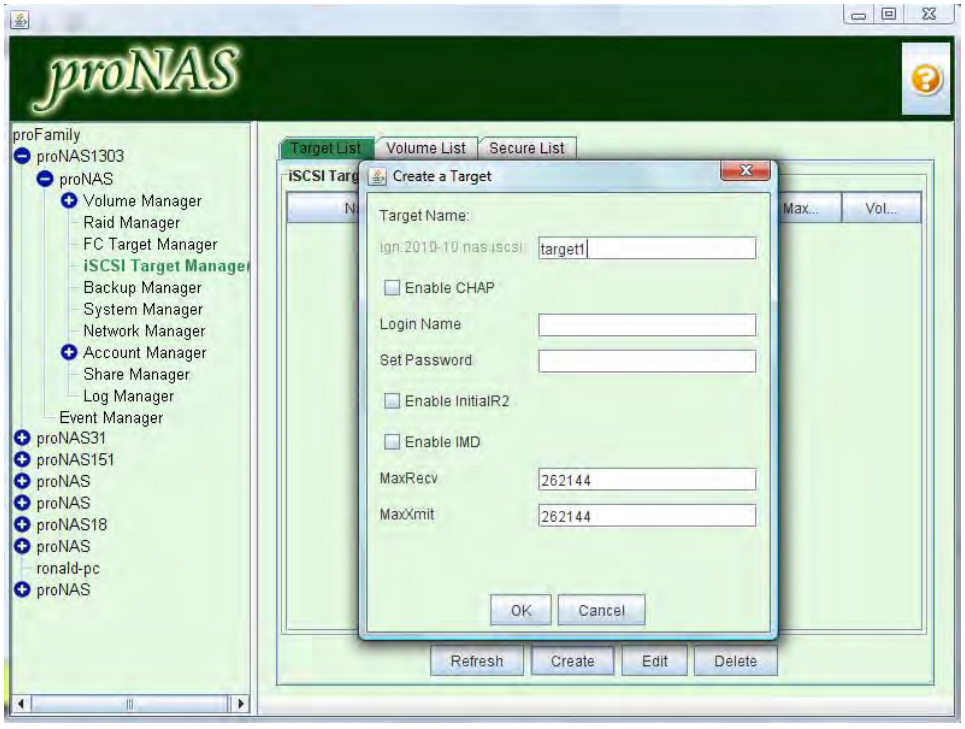
To create an iSCSI Target Name:

1. Select Target List and click “Create” button.

2. Enter a target name. If CHAP authentication is needed, tick “Enable CHAP” and enter the CHAP Login Name and Password.

NOTE: The first character in Target Name must be alphabet character; it cannot be numeric character.

If needed, tick the options “Enable InitialR2” (InitialR2T) and “Enable IMD” (ImmediateData).



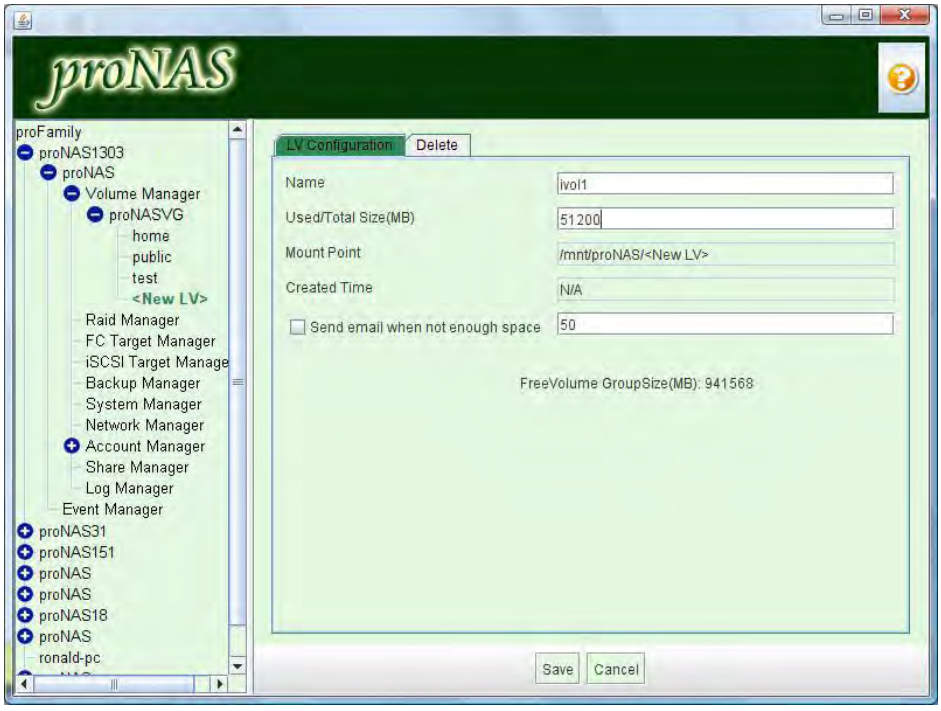
Target Name “target1”

3. Click “OK” to save. In confirm pop-up message, click “Yes” to confirm. The target name will appear in the Target List.

5.3.2 Volume List

The Volume List is used to create, edit, or delete iSCSI Target Volumes. This also shows the list of iSCSI target volumes.

NOTE: A Volume that will be used as iSCSI Target Volume must be created first in Volume Manager under a Volume Group (proNASVG, in this example), if one is not yet created.



Volume is created

To create an iSCSI Target Volume:

1. Click “Volume List” in iSCSI Target Manager.

2. Click “Create” button. The target name is shown. Select the volume from the Volume List (“vol1” in this example) that will be used as iSCSI target volume.

   Note that the LUN ID and Block Size settings will normally work and need not be changed.

3. Click “OK” when done. The iSCSI target volume will appear in the Volume List.

NOTE: An “i” icon on the left of the logical volume name (in Volume Manager) will appear. This denotes that iSCSI function is enabled on the volume.

5.3.3 Secure List

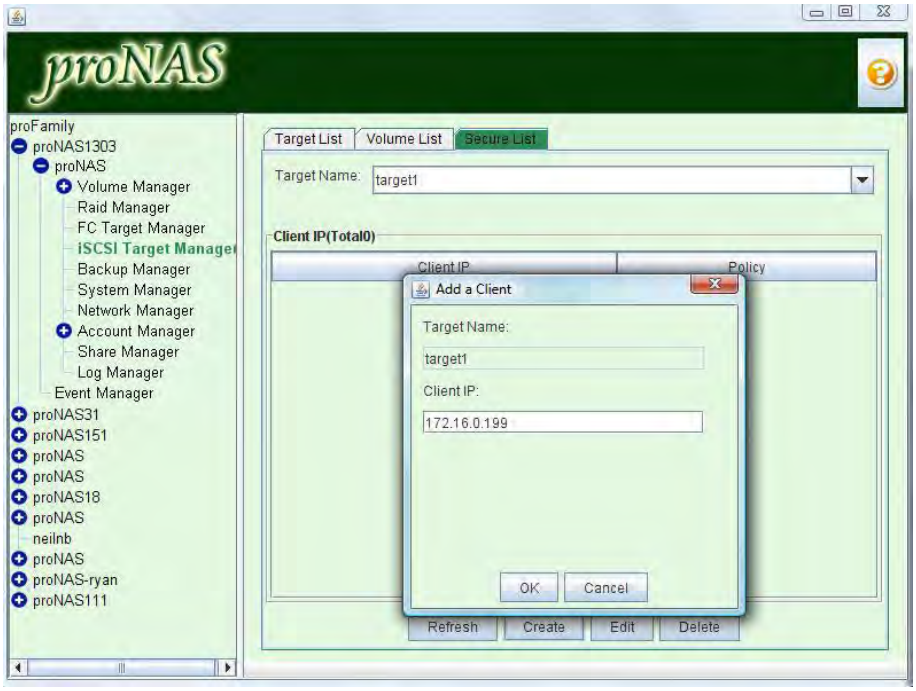
The Secure List is used to configure iSCSI target volume Host Filter, to allow certain hosts from accessing the iSCSI Target Volumes.

NOTE: By default, all clients are denied access to the iSCSI target volume.

To configure Secure List:

1. Select “Secure List”. Click “Create” to add IP of iSCSI host that will be allowed access to the iSCSI Target Volume.

   Enter the Client IP that will be allowed access.



2. Click “OK” when done. In Confirm pop-up message, click “Yes”. The Client IP will appear in the list.

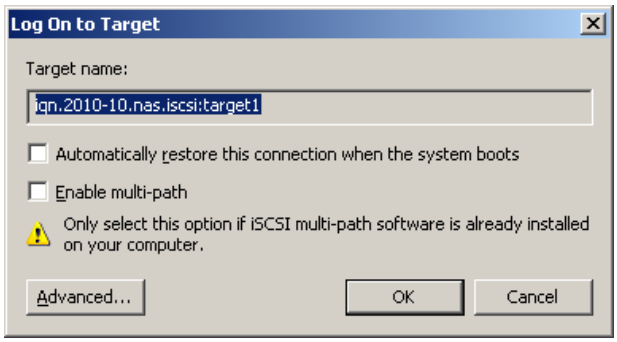
NOTE: Only one initiator (client IP) can access an iSCSI target volume. Only the client IP included in the list will be allowed access to the iSCSI target volume (LUN). Other clients will not see the LUN when connecting via iSCSI initiator.

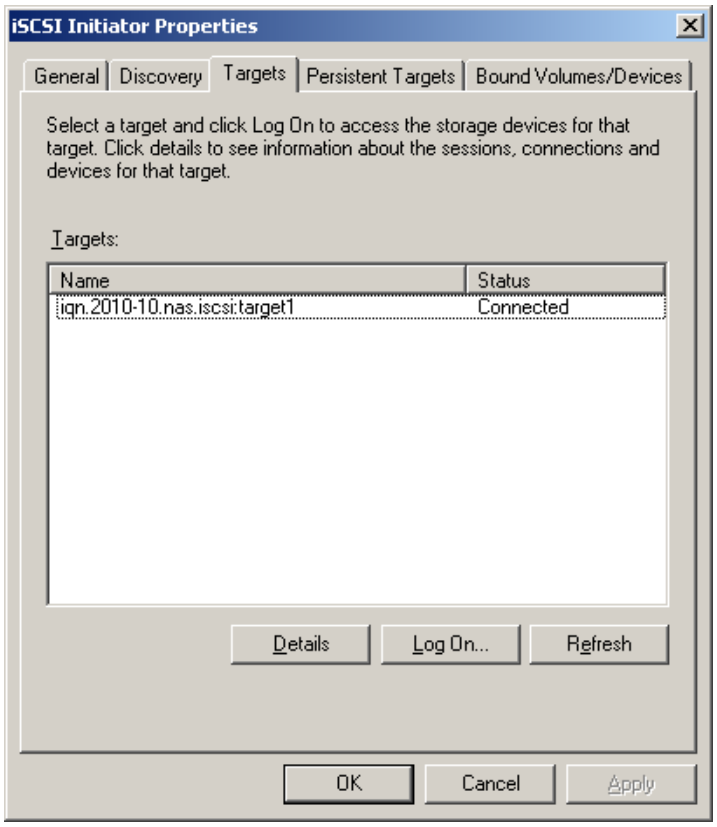
5.3.4 Connecting Host to iSCSI Target Volume

Example of connecting a host to iSCSI target volume using Windows iSCSI Initiator:

1. Open iSCSI Initiator in the Host computer that will connect to the ISCSI target volume.

2. Add the Target Portal IP in iSCSI Initiator and Logon.





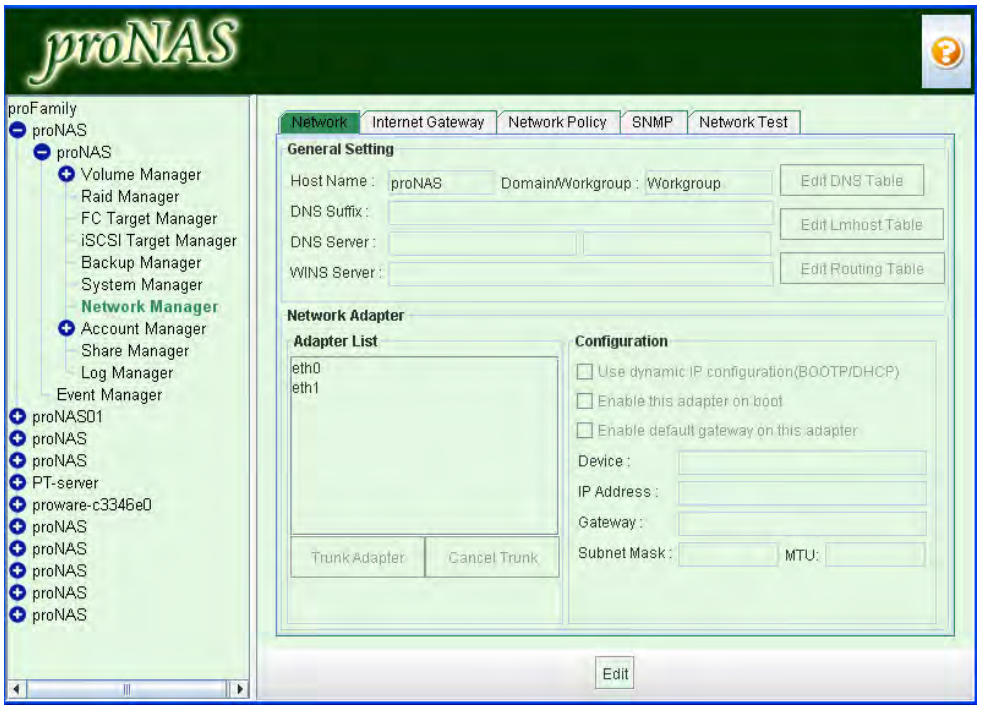
3. Initialize and format the disk device in Disk Management.

5.4 Network Manager

Using the Network Manager, you can configure the NAS network settings. There are five tabs in Network Manager: Network, Internet Gateway, Network Policy, SNMP, and Network Test.

5.4.1 Network Setting and Trunking

There are two sections in the Network tab, the General Setting section and the Network Adapter section.



The Network tab

Press “Edit” button to configure the Network settings and click “Save” button to update new settings.

General Setting:

- **Host Name -** The NetBIOS name of proNAS, it should be unique.
- **Domain / Workgroup** - Windows domain name or workgroup. Domain name is limited only up to 15 characters. For example: MYDOMAIN
- **DNS Suffix** - The DNS suffix appended to server name to complete the server’s FQDN. This includes the domain name, for example: MYDOMAIN.LOCAL
- **DNS Server** - DNS server is responsible for mapping the machine name and IP Address.
- **WINS Server** - WINS Server is responsible for the setting NetBIOS name resolution.

Edit DNS Table: If you have not set the DNS, you can use this button to edit DNS in the DNS table. This is optional.

Edit Lmhost Table: You can use this option to define the resolution of NetBIOS in the Lmhosts table. This is optional.

Edit Routing Table: You can use this option to define routing table. This is optional.

Network Adapter:

The Network Adapter section consists of the Adapter List and the Configuration section. The Adapter List is the list of available Ethernet ports in the system. The number of ports might be two or three depending on different models.

Adapter List: Lists the available Ethernet adapters.

Configuration:

- **Use Dynamic IP Configuration (BOOTP/DHCP) -** If checked, this specifies that this network connection will dynamically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server or from a Bootstrap Protocol (BOOTP) server.
- **Enable this adapter on boot** – If enabled, this adapter will be active when proNAS starts up.
- **Enable default gateway on this adapter** - If checked, the default gateway will be enabled in this adapter. A default gateway is a local IP router that is used to forward packets to destination beyond the local network. Only one default gateway can be enabled in a certain time.
- **Device** - Displays the type of Network Interface Card.
- **IP address** – Shows the current IP address. To edit IP address, enter the new IP address.
- **Gateway** – Shows the current gateway IP address. To edit, type in a new gateway IP address.
- **Subnet mask** – Shows the current subnet mask setting. To edit, type in the new subnet mask number.
- **MTU** – The MTU size (Maximum Transmission Unit) in bytes. To modify the MTU size for this interface, enter the new MTU size.

Network Trunking

ProNAS provides the network trunking/bonding function. Ethernet bonding refers to aggregating multiple Ethernet channels together to form a single channel.

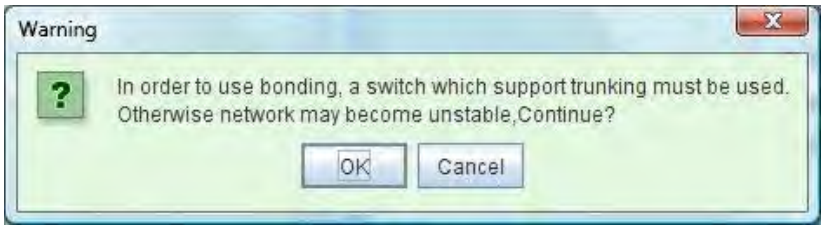
NOTE: It is necessary that the network switch supports the type of trunking mode that will be used. Otherwise, the network connections may become unstable.

5.4.1.1 Configure Network Adapter Trunking

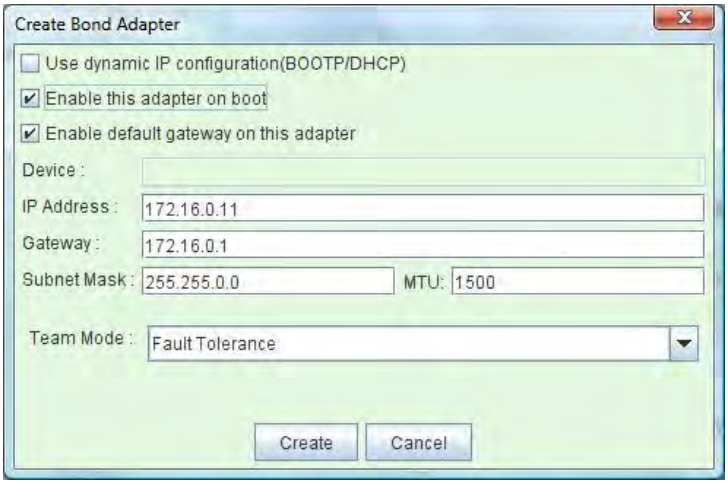
To create a trunk adapter:

- Click on the "Edit" button. Press the “Ctrl” key then at the same time select the adapters that will be included in the network trunking then click on "Trunk Adapter" button.

- A warning message will be displayed. Click “OK” to proceed.


Warning
In order to use bonding, a switch which support trunking must be used.
Otherwise network may become unstable,Continue?
OK
Cancel

o Setup the network settings. Select the Team Mode to use. Click “Create” when done.



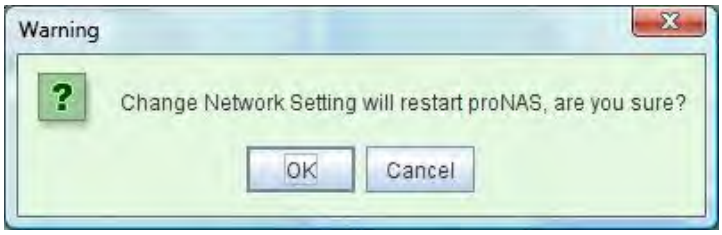
The Team Mode defines the type of operation for the bonded ports.

Team Mode options:

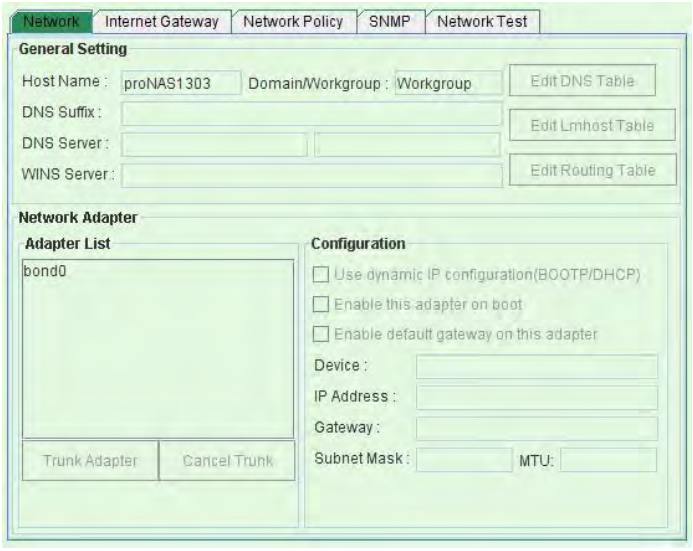
- **Fault Tolerant (Active_ Backup)** - Active_Backup policy: If the active Ethernet port fails, the standby Ethernet port will become active. This enhances the availability of access to the NAS.
- **Load balance and Fault Tolerant (XOR)** - XOR policy: Transmit based on source MAC address XOR with destination MAC address. This selects the same slave for each destination MAC address. This mode provides load balance and fault tolerance.
- **Link Aggregation (802.3ad)** - 802.3ad policy: Combines multiple physical network links into a single logical link for increased performance. Transmits and receives on all slaves in the active aggregator. Pre-requisite: the network switch must support IEEE 802.3ad.
- **Load Balance (ALB)** - ALB (Adaptive load balancing) policy: The receive load balancing is achieved by ARP negotiation and does not require special switch support.

4. Click “Save” to save the trunking configuration.

5. A warning message will be displayed. Click “OK” to continue.



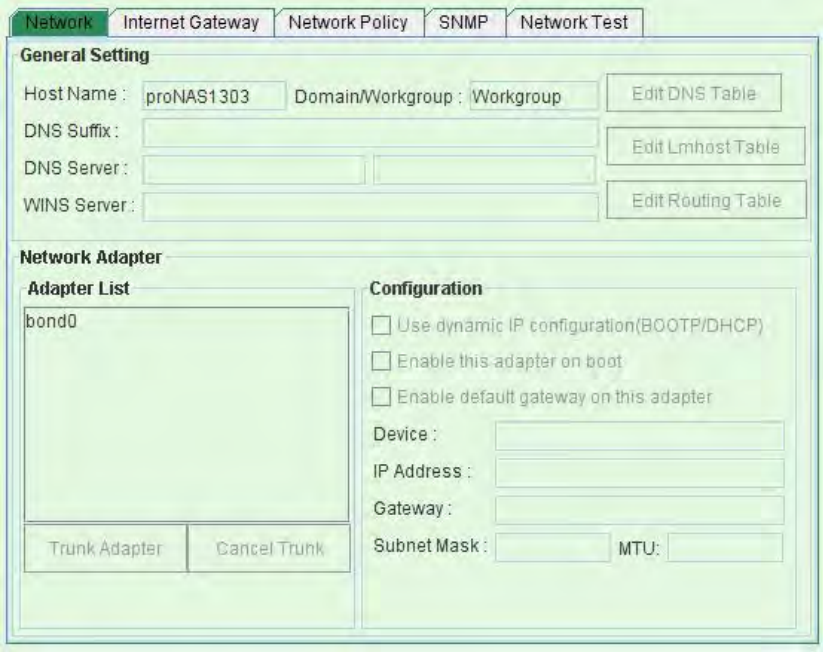
6. The network settings will be updated in a while. Connect to proNAS GUI using the new IP address used in network trunking. The Adapter List will show device “bond0”.



5.4.1.2 Cancel Trunking

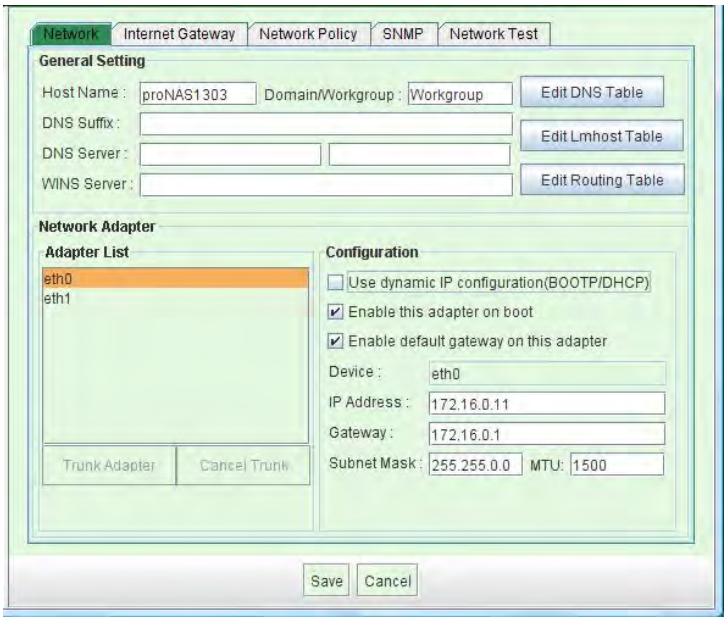
To cancel network trunking:

1. In Network Manager, Network tab, click “Edit” button.

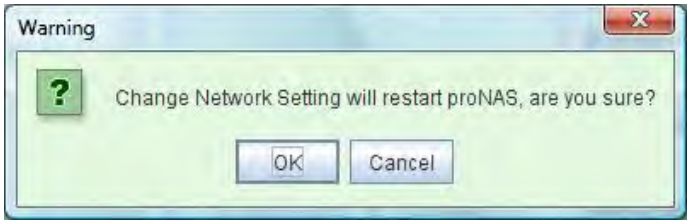


2. Select the bonding device “bond0” and click “Cancel Trunk”.

3. The original network adapters will appear. Network device “eth0” will be automatically assigned previous network settings of bond0. Modify the network settings if needed, then click “Save”.



4. A warning message will be displayed. Click “OK” to continue.



5. The network settings will be updated in a while, then re-login to proNAS GUI.

5.4.2 Internet Gateway

proNAS provides Internet gateway function which enables proNAS to act as an Internet Gateway, integrating DHCP service, routing and NAT. Using Internet gateway function, administrators can easily enable and disable the Internet access for network users.

To configure Internet Gateway, press “Edit” button.

Configuration options:

DHCP's IP range starting from - means the lower bound (starting) range of private IP addresses for DHCP

DHCP's IP range ending with - means the upper bound (ending) range of private IP addresses for DHCP

Private Net Adapter - means the port connected to private network. This port has to be a Static port and could also be a Trunk port.

WAN Adapter: means the port connected to WAN or Internet. This port could be a Trunk port.

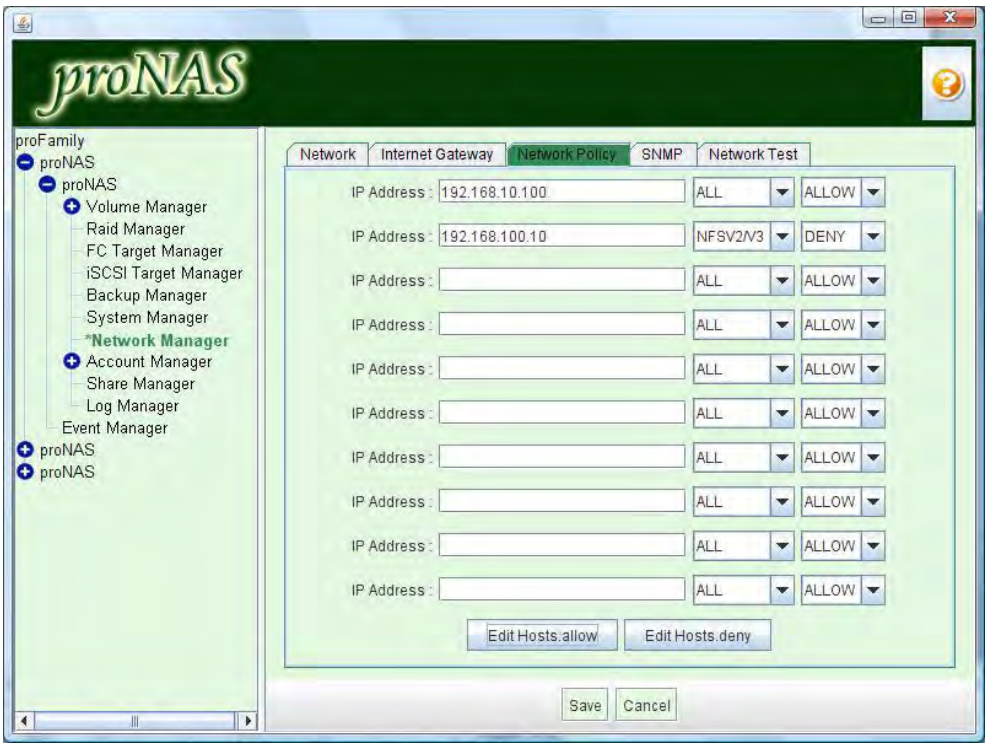
NOTE: When using Internet Gateway function, make sure the Internet Gateway service is enabled in the Service tab of System Manager.

5.4.3 Network Policy

Network Policy allows setup of Hosts (IP Addresses) access policy, such as allow or deny access to the NAS.

1. To setup Network Policy, click “Edit”.

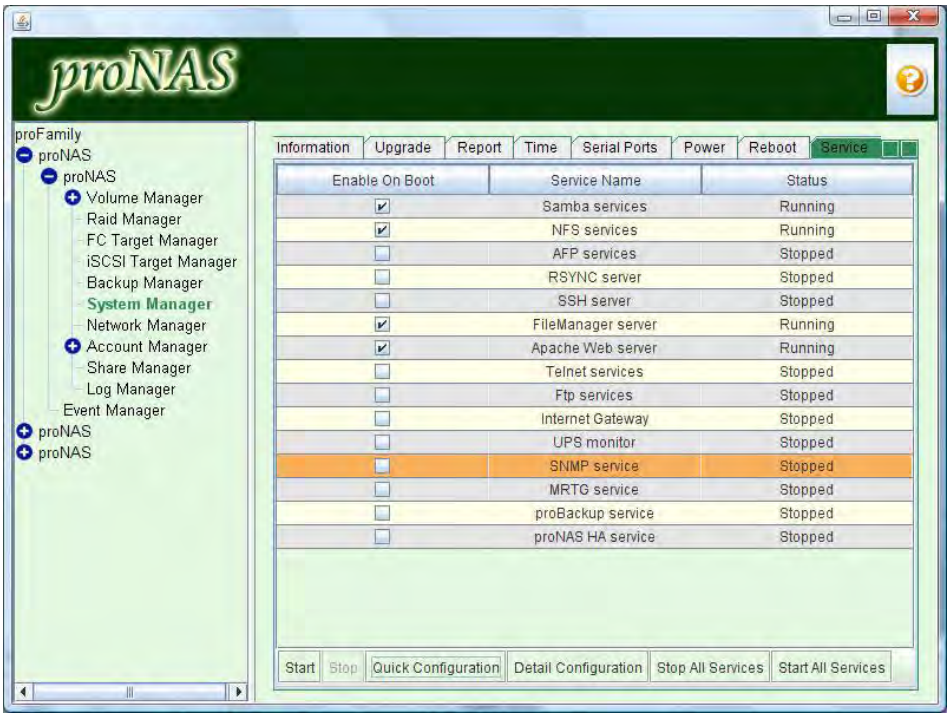
2. Enter the **IP address** or range of IP address that will be allowed or denied access. In the next column, select the **service** options such as NFSV2/V3, Telnet, FTP, and SSH. Default is “ALL” which means all service options (previously mentioned) are included.
   In the last column, select **access** option, “ALLOW” (the default setting) or change to “DENY” if necessary.
   When ALLOW is selected, the IP address is allowed access to the selected services. When DENY is selected, the IP address is denied access to the selected services.



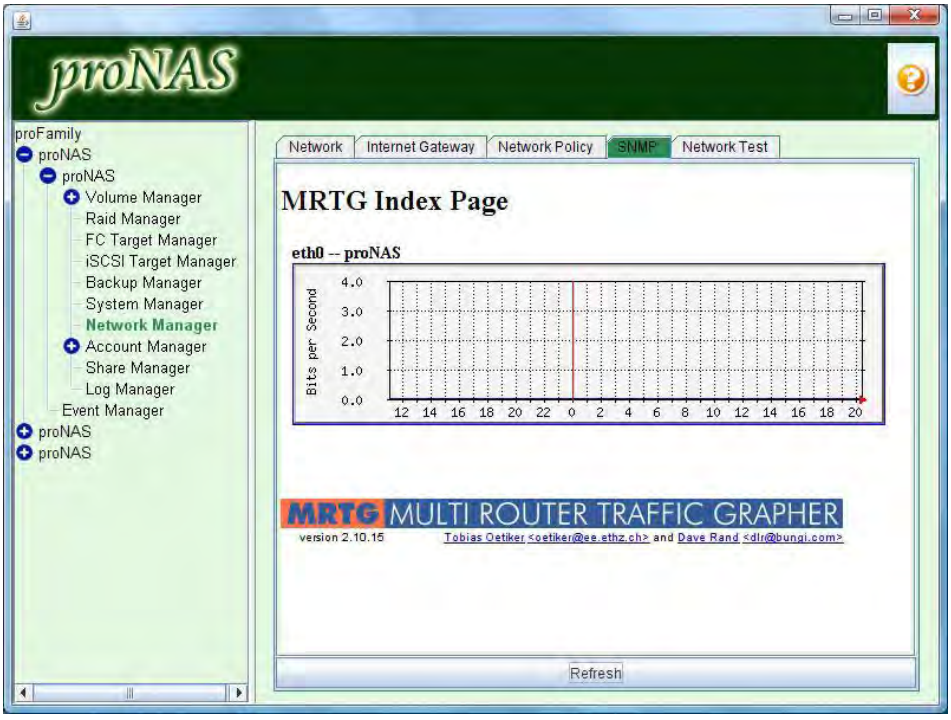
3. Click “Save” when done.

5.4.4 SNMP

The SNMP service can be enabled to monitor proNAS network traffic. Select Service tab of System Manager then enable **SNMP** service and **MRTG** service. Click “Start” to enable each service.



To view the SNMP network traffic information, select the SNMP tab in Network Manager.

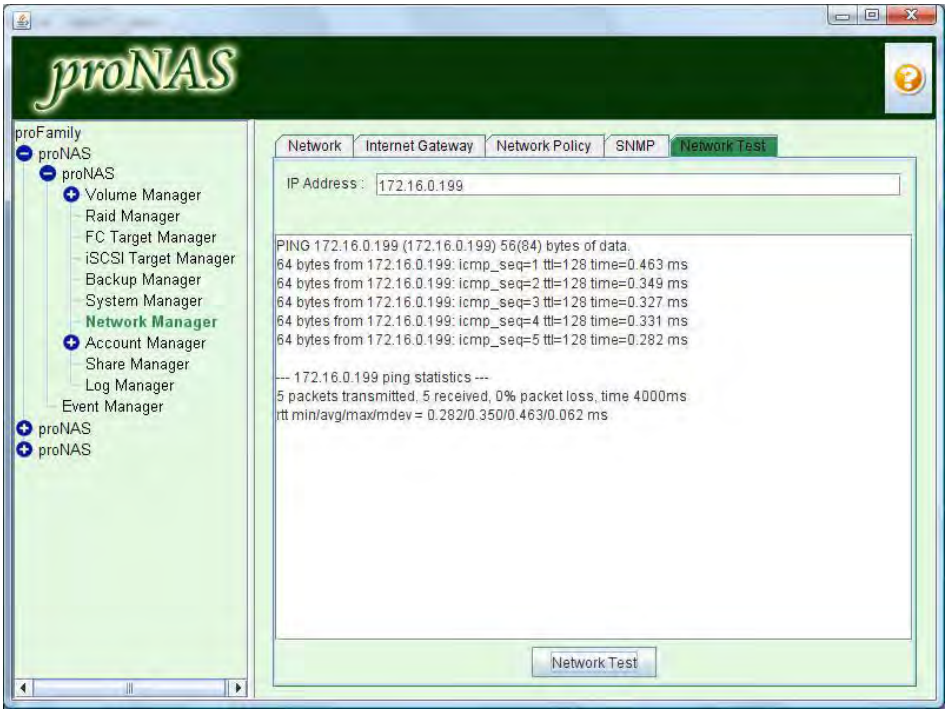


For more information about MRTG service, please visit http://www.mrtg.org.

5.4.5 Network Test

This function allows to test whether a particular host is reachable or to check connectivity to a particular IP address.

To test, enter the IP address in the IP address box then click “Network Test” button. The result will be displayed in the area below the IP address box.



5.5 Account Manager

With Account Manager, the administrator can manage and administer local accounts as well as import external domain accounts. proNAS will utilize external directory services to do account authentications which currently supports ADS/PDC and NIS.

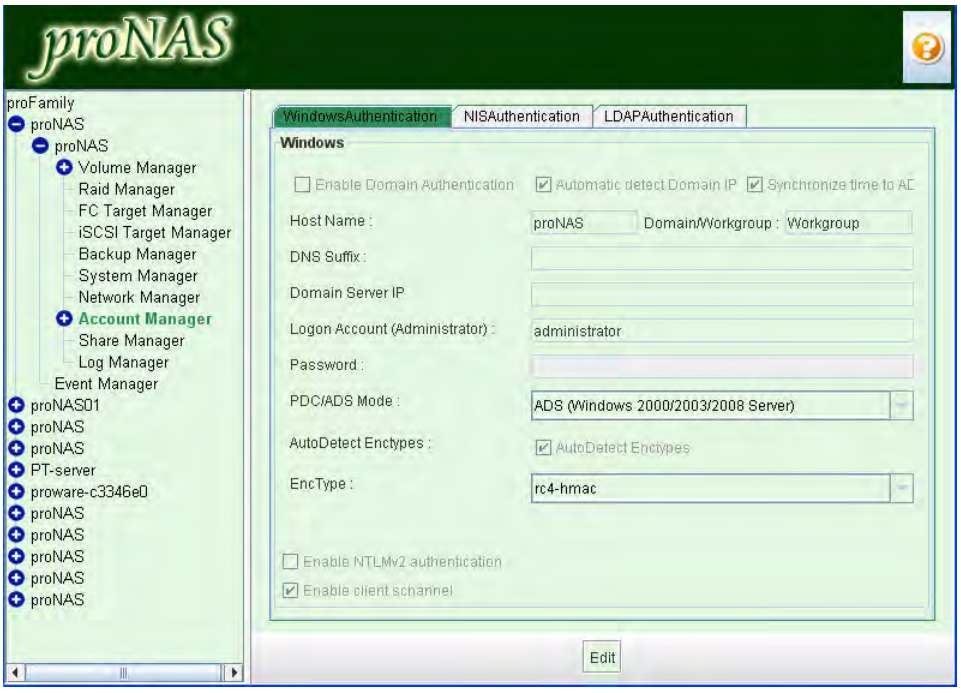
The main functions of the Account Manager are:

- Authentication
- User Account
- Group Management

5.5.1 External Accounts Integration (Domain Account Authentication)

You can utilize external directory services to authenticate accounts. Currently, **PDC/ADS**, **NIS**, and **LDAP** authentication are supported. Not allowed to setup different authentication option at the same time.

5.5.1.1 Windows Authentication



If you would like to integrate proNAS with Windows environment, please select “Edit” button then check "Enable Domain authentication". Set the necessary Windows options then click “Save” to update settings.

NOTE: Hostname, Domain name and DNS Suffix need to be set first in Network Manager.

Windows options:

- **Automatic detect Domain IP** – This is enabled by default. When enabled, proNAS will try to automatically detect the domain server's IP address.
- **Hostname** - Indicates the NetBIOS name of proNAS; must be set in Network Manager.
- **Domain / Workgroup** - Windows Domain name; must be specified in Network Manager.
- **DNS Suffix** - The DNS suffix used; must be set in Network Manager.
- **Domain Server IP** - The IP address of the domain server. proNAS will automatically acquire the domain server's IP address after setting the Domain name in Network Manager if "Automatic detect Domain IP" option is enabled. When "Automatic detect Domain IP" option is disabled, you need to manually enter the domain server's IP address.
- **Logon account (Administrator)** – the administrator's logon name in the Domain Controller
- **Password** - the administrator's password in the Domain Controller.
- **PDC / ADS Mode** – The type of Domain Controller. Choose PDC for Windows NT Server or ADS for Windows 2000/2003/2008 Server.
- **Auto Detect Enctypes** – This option automatically detects the encryption type used in Windows authentication. To manually select the encryption type, disable this option and select the preferred encryption type from the EncType drop-down list.
- **Enable NTLMv2 authentication** - This parameter determines whether or not smbclient will attempt to authenticate itself using the NTLMv2 encrypted password. If enable, proNAS will only sent NTLMv2 and LMv2 responses. NTLMv2 authentication protocol is available only on WindowsNT4 with SP4 and Windows 2000 or later. Default is disabled.
- **Enable client schannel** - This controls whether the client offers or even demands the use of the netlogon schannel. Default is auto, means it offers the schannel but does not enforce it.

5.5.1.2 Sample Steps to Join the NAS to Windows AD Domain:

1. Select Network Manager. In Network Manager –> Network tab, click “Edit” to configure network settings.

2. Change the default proNAS Host Name if there are other proNAS systems in the network. Enter the Windows Domain name in “Domain/Workgroup”. For example: MYDOMAIN

3. Enter the DNS Suffix.

NOTE: The DNS suffix is the name appended to the server name to complete the server’s FQDN. This includes the domain name. For example: MYDOMAIN.LOCAL

4. Enter the DNS Server and WINS Server (IP address) as necessary.

5. Click “Save”. The network settings will be updated in a while.

6. Select Account Manager. In Windows Authentication tab, click “Edit” button.

7. Tick “Enable Domain Authentication” option.

8. If the Domain Server IP is not detected (not shown), you can manually specify the Domain Server IP by removing the check mark in “Automatic Detect Domain IP” and entering the Domain Server IP address.

9. Enter the Domain Administrator Account and Password.

NOTE: No need to include “domain-name\” in Domain Administrator Account.

10. Select the Domain Server mode (PDC or ADS).

11. If needed, change the encryption type to the same type used by your domain server.

12. Click “Save”. The NAS will be joined to Windows Domain in a while.

13. To verify, select Account under Account Manager; the domain user accounts should be displayed. You can also verify domain group accounts in Group List.

5.5.1.3 NIS Authentication

If you would like to integrate proNAS with UNIX/Linux environment, please select “NIS Authentication” tab and click “Edit” button then check "Enable NIS authentication". Set the necessary configuration options then click “Save” to update settings.

Configuration Options:

- **NIS Domain** - Enter the NIS domain name
- **NIS server** - Enter the IP Address of NIS server.

5.5.1.4 Sample Steps to Join NIS Domain:

1. Under Account Manager, select NIS Authentication tab. Click Edit.

2. Check the Enable NIS Authentication option. Enter the NIS Domain name (e.g.: TESTDOM.LOCAL) and NIS Server IP address or FQDN. Click Save when done.

3. Click Account under Account Manager to verify that the NIS Accounts are listed in the Account List, or select Group to display the NIS Groups in the Group List.

5.5.1.5 LDAP Authentication

If you would like to enable authentication using LDAP (Lightweight Directory Access Protocol), select “LDAP Authentication” tab and click “Edit” button then tick "Enable LDAP Authentication". Set the necessary configuration options then click “Save” to update settings.

Configuration Options:

- **LDAP server DC suffix** - the LDAP DC (domain component) suffix
  Example: dc=ldapserver,dc=com
- **LDAP server IP address** - the IP Address of LDAP server
- **LDAP admin DN** - the admin account’s DN (Distinguished Name)
  Example: cn=admin,dc=ldapserver,dc=com
- **LDAP admin password** - the admin account’s password

5.5.1.6 Sample Steps to Setup LDAP:

1. Under Account Manager, select LDAP Authentication tab. Click Edit.

2. Check the “Enable LDAP Authentication” option. Enter the LDAP server DC suffix (example: dc=rdldap, dc=com), LDAP server IP address, LDAP admin DN, and LDAP admin password. Click “Save” when done.

3. Click Account under Account Manager to verify that the LDAP user accounts are listed in the Account List.

proNAS
proFamily
proNAS1303A
proNAS
Volume Manager
proNASVG
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Group
Account
Share Manager
Log Manager
Event Manager
proware-c3346e0
Account List
Total: 11
Login Name | Full Na... | Quota(... | Directory Serv... | Usa... | Stat...
nobody | Nobody | 0 | local | 1 | Disable
admin | Administrator | 0 | local | 0 | Enable
ldapuser1 | ldapuser1 | 0 | ldap | 0 | Enable
judy | judy | 0 | ldap | 0 | Enable
lady | lady | 0 | ldap | 0 | Enable
grace | grace | 0 | ldap | 0 | Enable
keigo | keigo | 0 | ldap | 0 | Enable
keigo1 | keigo1 | 0 | ldap | 0 | Enable
aaa | aaa | 0 | ldap | 0 | Enable
rocky | rocky | 0 | ldap | 0 | Enable
gaga | gaga | 0 | ldap | 0 | Enable
Create
Enable
Disable
Delete
Import Accounts
Refresh

5.5.2 Local Account and Group Management

Account Management

The Account List in Account Manager displays Local users and External users, ADS/PDC or NIS.

In Account menu, admin can perform the following functions:

- Create a new Local Account
- Enable and Disable an Account
- Modify and Delete an Account
- Mass Import Accounts
- Refresh the Account List

Creating a new Local account

Following are the steps to create a new Local account:

1. Select Account Manager in the proFamily tree. Choose Account node under the Account Manager. It will display all accounts under the Account List tab.

2. Press the "Create" button. System will display "Account List tab". Account List tab consist of two tabs, "Properties" and "Permission". In the Properties tab, enter the necessary information.

General:

- **Login Name** - Input the login name, it should be unique in proNAS
- **Full Name -** the complete name of the account
- **Directory Service -** system will display if the directory service is Local or ADS/PDC,NIS
- **Create Date -** system will display the create date of the account.
- **UID -** In UNIX/Linux, OS will assign a unique user number called UID to access the system resource. (UID range is 1 to 65535). proNAS may either assign a new UID automatically starting from 500 or you can manually specify the UID. Domain accounts will have a UID starting from 10000-30000.
- **Quota Size (MB)** – Use this to assign quota (usable space) to the user for his "home" folder. The default is 0, which means user has no limit in his home folder. The limit then is the size of the "home" volume.

NOTE: The setting for "Quota (MB)" when creating or editing a user account applies only to the "home" folder of the user account. This is different from the user account's quota for other share folders. The setting of a user account quota for a share folder is done in the Share folder itself, in the Privilege tab.

- **Set it to default value for new account** – When this option is enabled and the Quota Size value has been changed from 0 to another value, the new value set in Quota Size will become the new default Quota Size when other accounts are created.

- **Set Password** – Click this button to set the account's password. Passwords have to be at least 6 characters.

Status:

- **Current status:** Displays Enable or Disable.
- **Used Size (MB):** Displays the current used size.

Use the following guidelines to ensure that you are using a valid Account name:

- Account names must start with a small alphabet letter.
- Account names cannot be longer than 32 characters.
- Account names should be unique. No account names must be the same. No account names must be the same with share names.
- Account names cannot contain blank spaces.
- Account names cannot begin with a dash (-) and cannot consist of only a single dash.
- Account names cannot contain the following characters: /\[]";:|<>+=,?*
- Account names cannot be duplicated with the system default accounts, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. After completing the settings, press the "Save" button to save settings; or you may go to "Permission" tab to have a look at the permissions of the account then click “Save” button when done.

Permission tab

- **Joined Groups:** The account has gained access right because of joining certain groups.
- **Individually Authorized Shares:** Implies that the account has gained access rights individually.
- **Ownership:** Implies that the account has gained access right because it is the owner.

NOTE: A newly created local user account is automatically a member of the local "users" group.

Enabling and Disabling an Account

Account Manager allows the administrator to enable or disable a user account. When an account is disabled, the account cannot be used to login and access proNAS.
To forbid certain user account in accessing proNAS, highlight the account then press "Disable" button. The account will be shown with “Status” as Disable. If you would like to re-enable the user account proNAS, press "Enable" button. Disabling account "admin" is not allowed as well as all ADS/PDC and NIS accounts.

Deleting an Account

If you would like to delete a certain account, highlight the account then press "Delete" button. The user's home directory will be deleted. If the user owns one of the share, the owner of that share will be set to "admin". Account "admin" is not allowed to be deleted as well as ADS/PDC and NIS accounts.

Modifying an Account

If you want to modify an account, double-click on the account. You can only modify the password and permissions. If the account is an external domain account (created by ADS/PDC or NIS domain server), the account and password can not be modified in proNAS Account Manager. In such a case, you can only modify the permissions.

Importing of Accounts

proNAS provides Import Account function for creating large number of accounts instead of adding an account one by one. Administrator can create multiple user accounts in a text file with the following format: UID, Logon Account, Logon Password, Full Name. Example:

1019, david, proware, David Huang

1020, rocky, proware, Rocky Lee

To import the accounts, click on "Import Accounts" button then select the text file.

NOTE: The information for each account must start on a new line. If account creation fails for any account, proNAS skips that line (of account information) and continues with the next line.

Refreshing the Account List

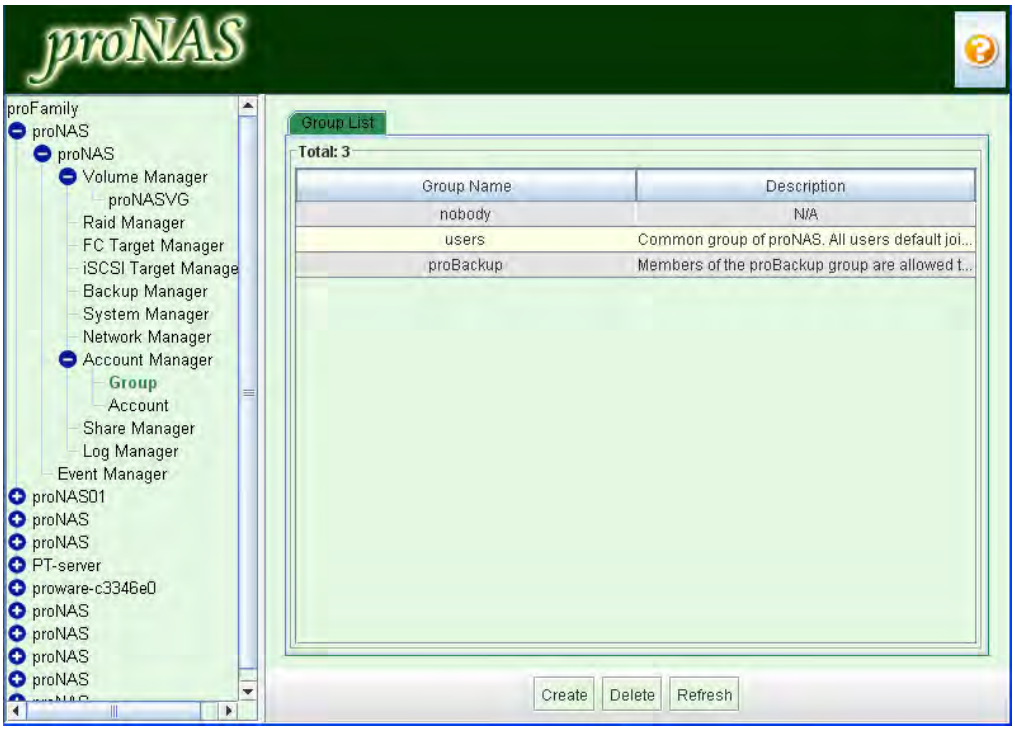
Use the “Refresh” button to automatically synchronize any new accounts created in ADS/PDC or NIS domain.

Group Management

Using group management, admin can organize access to proNAS shares. For example, a Sales group can be created for the sales department and this group can be assigned read-write access to the Sales Report share. All account members of the Sales group can have access to the Sales Report share.

Group List tab

The Group List tab shows the Local and External (ADS/PDC or NIS) Groups.



Group management allows the administrator to:

- Create or Delete a Local group
- Modify a Group
- Refresh the Group List

proNAS has two default groups, "users" and "proBackup". Every local user that will be created will automatically become a member of users group. proBackup group is used by proNAS for the proBackup service.

Creating a new Local Group

When a Local Group is added, it is created in the local account database of NAS. One account can become a member of more than one group.

Following are the steps to create a new Local Group:

1. Select Account Manager in the proFamily tree. Choose Group node under the Account Manager. It will display all groups under the Group List tab. Press the "Create" button.
2. Enter the necessary information. Refer to options below.

Create Group Options:

- **Group Name** - Enter the name of new group. It should be unique.
- **GID** - Group ID. proNAS will either automatically assign a GID when you create a group, or you can manually specify a GID.
- **Description** – Additional information or description about the Group can be entered here.

Account List – shows the list if accounts that are available and can be joined to the group

Current Member(s) – shows the list if accounts that are currently member of the group

NOTE: AD domain accounts cannot be joined to local groups.

Use the following guidelines to ensure that you are using a valid Group name:

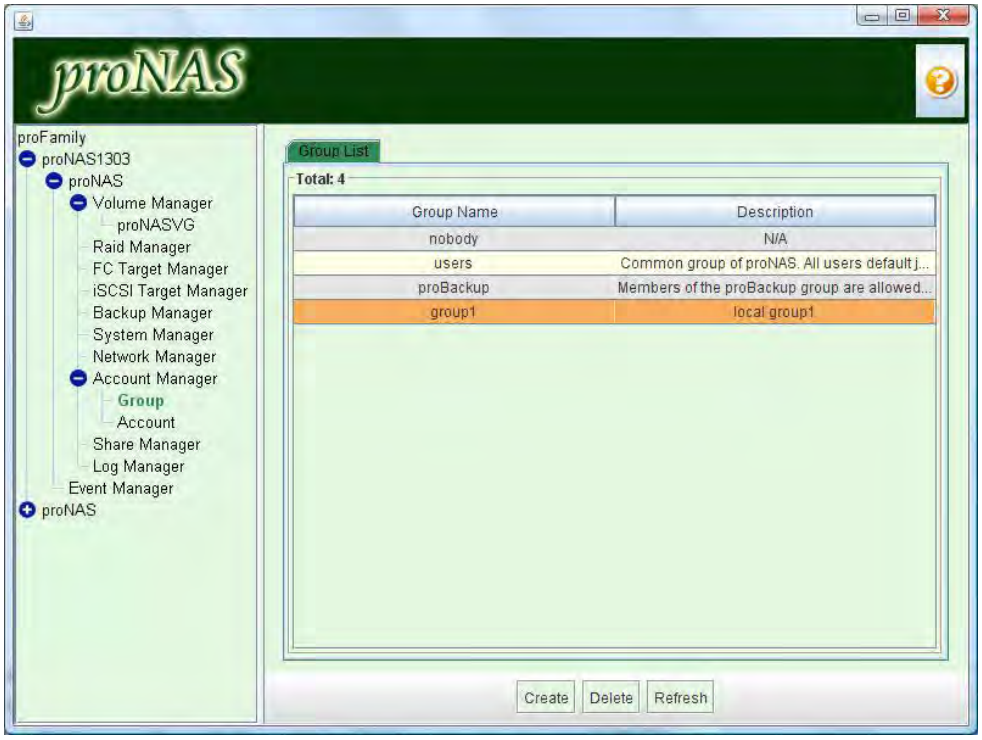
- Group names cannot be longer than 16 characters.
- Group names should be unique. No group names must be the same.
- Group names cannot contain blank spaces.
- Group names cannot begin with a dash (-) and cannot consist of only a single dash.
- Group names cannot contain the following characters: /\[]";:|<>+=,?*
- Group names cannot be duplicated with the system default groups, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. In the Account List, select the account(s) that will be joined to the group then click the "**>>**" button. The accounts will appear in the Current Member(s) list. To remove an account from the group, select the account in Current Member(s) list then click "**<<**" button.

4. Click "Save" button to save settings.

Deleting a Local Group

To delete a group, select the group to be deleted and then click the "Delete" button. ADS/PDC and NIS groups are not allowed to be deleted. Default group "users" and "proBackup" cannot also be deleted.



Modifying a Group

To modify a group, double click the group in Group List tab. The "Group List" tab will be displayed in edit mode. Group name, description, group members are allowed to be modified however this is only applicable to local groups. ADS/PDC and NIS groups are not allowed to be modified. Default group "users" and "proBackup" cannot be modified. ADS/PDC and NIS domain accounts are also not allowed to be joined to any local group except to "proBackup" group.

Refreshing the Group List

Use the “Refresh” button to automatically synchronize any new groups created in ADS/PDC or NIS domain.

5.6 Share Manager

In proNAS Share Manager, you can create and configure a Share, assign a share owner, assign user permission, and specify file sharing protocol. Under this node you can also use duplication function and rsync utility. Duplication is a share function in which you can replicate your share into another share using file level replication. Rsync utility is used to copy files either to or from a remote host, or locally on the current host.

In the "**Share List**" tab, you can see the list of current shares and it also displays share information such as share name, quota, used space, logical volume and share owner. There are 2 Default Share in proNAS: "home" and "public".

Share folder gets created under a logical volume. Make sure that an LV is already created before creating the share folder or admin can create the share folder and LV simultaneously, which can be done using the option “Create New Volume” in Properties tab of Share Manager.

Share Manager – “Options” tab

The Options tab is used to enable the Recycle Bin option or the Audit option.

The **Recycle Bin** function allows temporary storage of deleted files accessed via CIFS.

The **Audit** function allows saving audit log for share folders accessed via CIFS.

Please refer to more detailed information how to use Recycle Bin and Audit in the succeeding sections 8.6.8 and 8.6.9 respectively.

5.6.1 Share Management

5.6.1.1 Creating a New Share

To create a new share folder:

1. Select Share Manager then press "Add New Share" button.
2. Configure all necessary share options in Properties, Protocol, and Privilege tabs. Refer to Properties Setting, Protocol Setting, and Privilege Setting Sections in the succeeding pages.
3. Click “Save” button to save the settings.

NOTE: After creating the share and setting the Properties, Protocol and Privilege tabs, you can go back to these tabs and modify the various options. To edit, click the share name in Share Manager and click “Edit” button.

5.6.1.2 Applying ACL

When applying ACL in a share, **all the files and subfolders under this share will inherit the share's permission**. "Apply ACL" will propagate the ACL (permission) settings of the share folder into all of its child directories and files. For example, if user1 has read/write permission on the sub-folder but read only on the share, after applying ACL, user1 will now have a read-only permission on the sub-folder.

5.6.1.3 Modifying a Share

After creating the share, you can modify the Properties, Protocol, and Privilege tabs, as well as setup the Rsync and Duplication functions. Click the “Edit” button to modify the share.

5.6.1.4 Deleting a Share

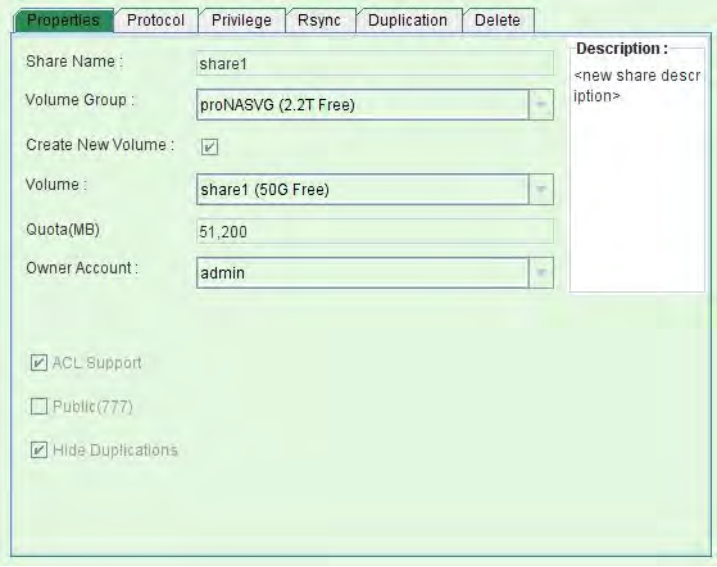
If you delete a share, all the data in the share is deleted. If the data in the share is no longer needed or a backup of the data has been made, you may delete a share. If backup has not been made yet and data in the share is still needed, make a backup first before deleting the share.

5.6.2 Properties Setting

The Properties tab contains the following settings:

- **Share Name -** Input the share name, it should be unique in proNAS.
  Use the following guidelines to ensure that you are using a valid Share name:
  - Names cannot be longer than 31 characters.
  - Names should be unique. It cannot be a duplicate with other LV names, shares, and Account names.
  - Names cannot contain blank spaces.
  - Names cannot begin with a dash (-) and cannot consist of only a single dash.
  - Names cannot contain the following characters: /\[]";:|<>+=,?*

- **Volume Group (VG)** - Choose a volume group from the list. Only Volume groups that has member disk will be displayed. System will also display the available space of the volume group.
- **Create New Volume (LV)** -If you check this option, system will create a new LV as well as create the new Share. The LV name will be the same as the share name.
- **Volume -** Select a logical volume from the selected volume group.
- **Quota (MB) -** Input the size of the share. This is also the size of the logical volume to be created if you choose to create an LV at the same time.
- **Owner Account -** Specifies the owner of the share.
- **ACL Support** – Specifies if the share will support ACL permission (option is enabled by default) or support “chmod” permission.
- **Public (777)** - This option allows you to set a share as a public share. When enabled, any user within the specified private net can connect to this share.
- **Hide Duplications** - This option allows you hide or unhide the "_Duplication" folder in this share. The default will be hidden.



5.6.2.1 Steps to Make a Share Folder a Public Folder Accessible to All Users:

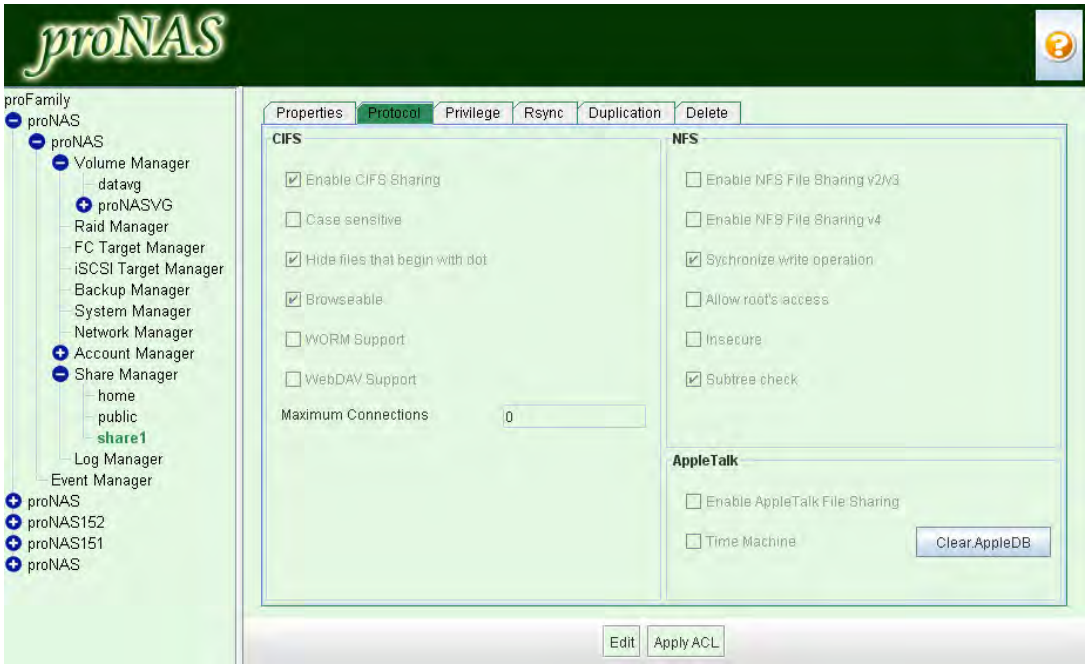
NOTE: It is not recommended to set a Share as a Public Share folder. Any local NAS account or Windows/NIS domain account (if NAS is joined to the domain) can login to the share with Read/Write privilege.

1. Select Share Manager. Select the share name that will be made accessible to all users.
2. In the Properties tab, click “Edit”. Select (tick) the “Public (777)” option.
3. Click “Save”. When a warning message is displayed, click “OK” to proceed.

NOTE: If you need to reassign ACL, click “Edit” then enable (check) the “ACL Support” option. The “Public (777)” option will be automatically disabled (unchecked).

5.6.3 Protocol Setting

ProNAS supports the following share protocols: CIFS, NFS, and AppleTalk which can be set in Protocol tab when creating the share or when in edit mode.



5.6.3.1 CIFS

- **Enable CIFS Sharing** - This option is used to enable or disable CIFS sharing. By default, this option is enabled. MS Windows clients usually use CIFS to connect to this share. Note that newer versions of Mac OS X also support CIFS share connection and does not need to enable/use AppleTalk.
- **Case sensitive** - This control whether filenames are case sensitive.
- **Hide files that begin with dot** - This option controls whether files starting with a dot will be hidden.
- **Browseable** - This option controls whether the share folder name will be shown and can be browsed when connecting to NAS. Default setting is enabled. For example, if this option is disabled (unchecked) and a client PC connects to the NAS via CIFS (with the option “Enable CIFS Sharing” enabled in the share), the share will not be visible.
- **WORM Support** - This allows data to be written once to a share folder, and prevents data to be erased. After data is written, it will become read-only.
- **WebDAV Support** - This allows users to access their data through the web using HTTP protocol.
- **Maximum Connections** - This option limits the number of simultaneous connections at a certain time. Default value is zero, which means an unlimited number of simultaneous connections are possible in this share.

NOTE: The default setting of "Maximum Connections" is 0. If there is a need to limit the number of simultaneous connections to a CIFS share, set it to specific number instead of 0.

5.6.3.2 NFS

- **Enable NFS file sharing v2/v3** - This specifies whether to enable or disable NFS version 2 / version 3 file sharing. NFS is used in UNIX/Linux environment.
- **Enable NFS file sharing v4** - This specifies whether to enable or disable NFS version 4 file sharing.
- **Synchronize write operation** – Use this option to enable or disable write caching
- **Allow root's access** – Use this option to allow or disallow access by root super user account
- **Insecure** - If you choose this option, it means only the port under 1024 can access, it provides higher security
- **Subtree check** – Use this option to enable or disable subtree checking. A subtree check happens if a subdirectory of a filesystem is exported, but the whole filesystem isn't then whenever a NFS request arrives, the server must check not only that the accessed file is in the appropriate filesystem (which is easy) but also that it is in the exported tree (which is harder).

Accessing proNAS shares under Linux

For NFS share:

Usage: mount -t nfs x.x.x.x:/mnt/proNAS/volume/share /mnt/temp

Where:

x.x.x.x = proNAS IP address

/mnt/proNAS/volume/share = the complete path of the NFS share. You may use the command "showmount -e x.x.x.x" to query the complete path.

/mnt/temp = local mount point on the client

For CIFS share:

Usage: mount -t smbfs //x.x.x.x/share /mnt/temp -o username=account,password=secret

or

mount.cifs //x.x.x.x/share /mnt/temp -o username=account,password=secret

or

smbmount //x.x.x.x/share /mnt/temp -o username=account,password=secret

where:

x.x.x.x = proNAS IP address

share = CIFS share name. You may use the command "smbclient -L x.x.x.x" to query the CIFS share names.
/mnt/temp = local client mount point.
-o username=account,password=secret = the account name and password

5.6.3.3 AppleTalk

Enable AppleTalk File Sharing: This specifies whether to enable or disable AppleTalk file sharing (AFP). When enabled, the share folder can be accessed via Appletalk (AFP).

Note that newer Mac OS X versions support SMB protocol, and therefore will be able to connect to NAS share folder using SMB protocol, without enabling AppleTalk (AFP).

Time Machine – Used this option to enable Time Machine function on the share folder. The NAS share folder will become Time Machine backup target destination.

Clear .AppleDB – Use this button to delete the .AppleDB hidden folder (including all files in it) on the share folder.

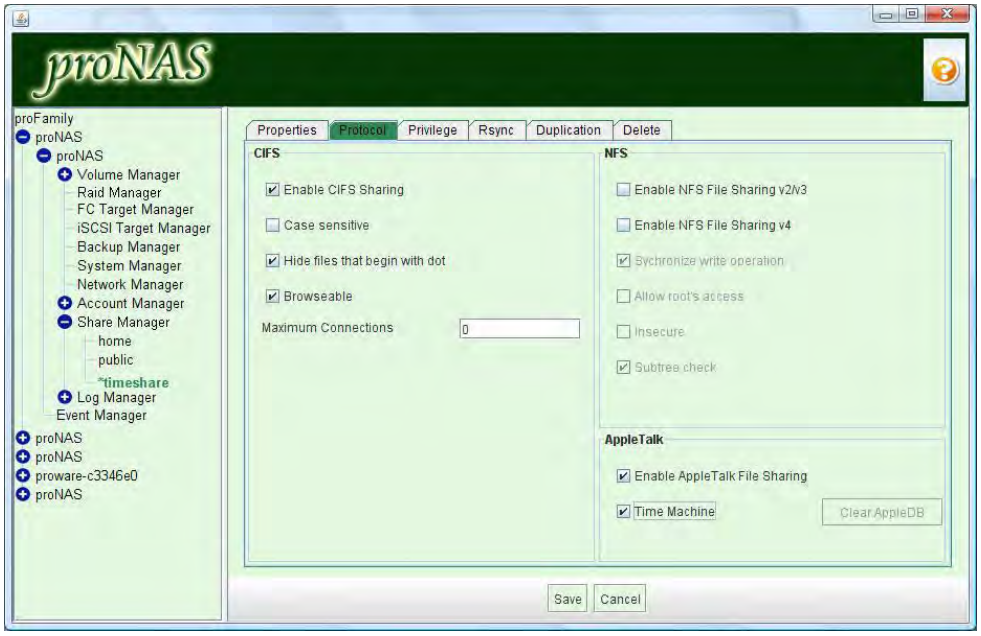
5.6.3.4 How to Setup Time Machine

The NAS supports Time Machine to backup data from Mac to NAS share folder automatically. For more information about Time Machine, please visit Apple's website at http://www.apple.com/macosx/what-is-macosx/time-machine.html

To setup Time Machine:

1. In Share Manager, edit an existing share or create a new share (in this example, it is named "timeshare") for Time Machine use.

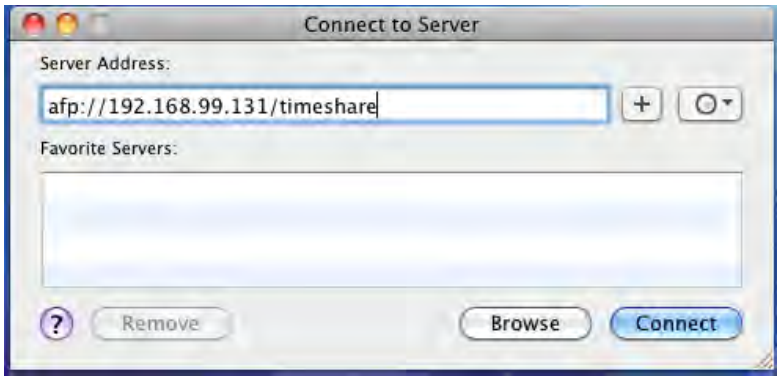
2. In the Protocol setting, in AppleTalk pane, tick both the “Enable AppleTalk File Sharing” and “Time Machine” options. Click “Save”.



3. In System Manager, Service, make sure the “AFP services” is Running. If not, start the service.

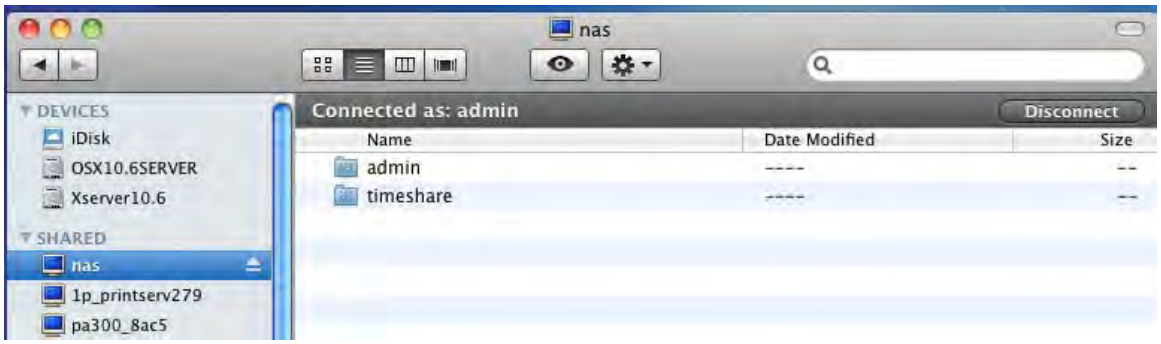
4. On Mac machine, to login to the NAS share folder via AFP, select “Go” then “Connect to Server”.

5. In Server Address, enter “afp://x.x.x.x/timeshare”, where x.x.x.x is the NAS IP address and timeshare is the share folder previously configured for Time Machine use. Then click “Connect”.



6. Enter a valid Account Name and Password; use account which has permission to the NAS share folder. In this example, admin account is used. Then click “Connect”.

7. The Mac will be connected to the NAS share folder.



8. To setup Time Machine in Mac, open Time Machine.

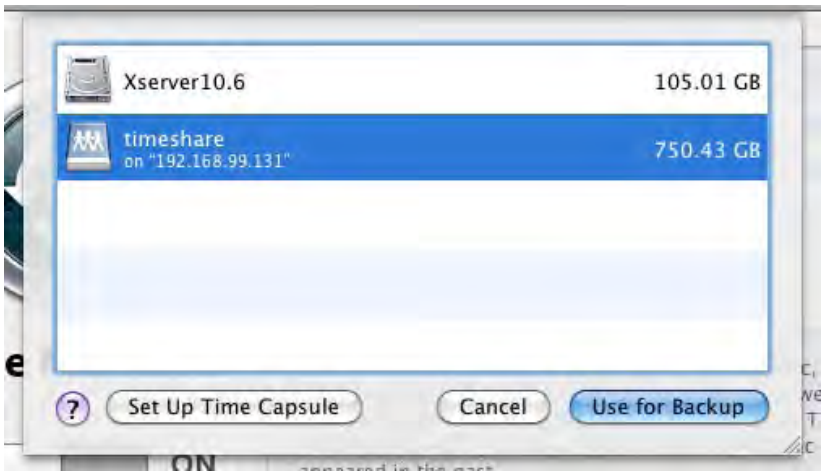
9. If the Time Machine has not been previously setup, a message will be shown as below. Then select “Set Up Time Machine”.

You haven't selected a location for Time Machine backups.
To select a location for backups, set up Time Machine.
Cancel
Set Up Time Machine

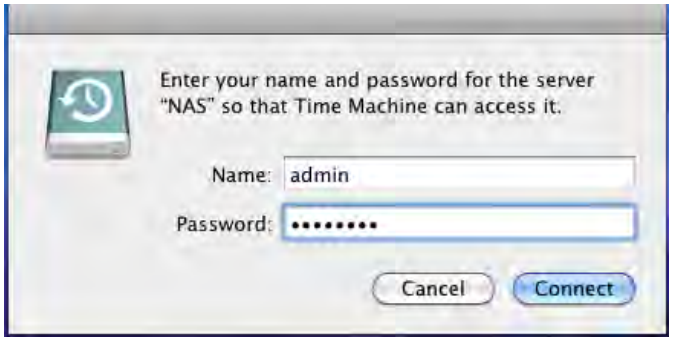
10. The Time Machine screen will be displayed. Click “Select Backup Disk…”.

Time Machine
Show All
Select Backup Disk...
Time Machine
OFF
ON
Time Machine keeps copies of everything on your Mac, including system files, applications, and settings, as well as your music, pictures, and other important files. Since Time Machine keeps daily backups, you can revisit your Mac as it appeared in the past.
Show Time Machine status in the menu bar
Click the lock to prevent further changes.

11. Select the “timeshare” disk and click “Use for Backup”.



12. Enter the account user name and account password to access the NAS share folder via Time Machine, and then click “Connect”.



13. After successful connection, the Time Machine is setup. The available space on the NAS share folder will be shown. The Next Backup time is also displayed.

Time Machine
Show All
Name: timeshare
Available: 750.43 GB of 751.49 GB
Oldest Backup: --
Latest Backup: --
Next Backup: 110 seconds
Select Disk...
Options...
Time Machine
OFF
ON
Time Machine keeps
• Hourly backups for the past 24 hours
• Daily backups for the past month
• Weekly backups for all previous months
The oldest backups are deleted when your disk becomes full.
Show Time Machine status in the menu bar
Click the lock to prevent further changes.

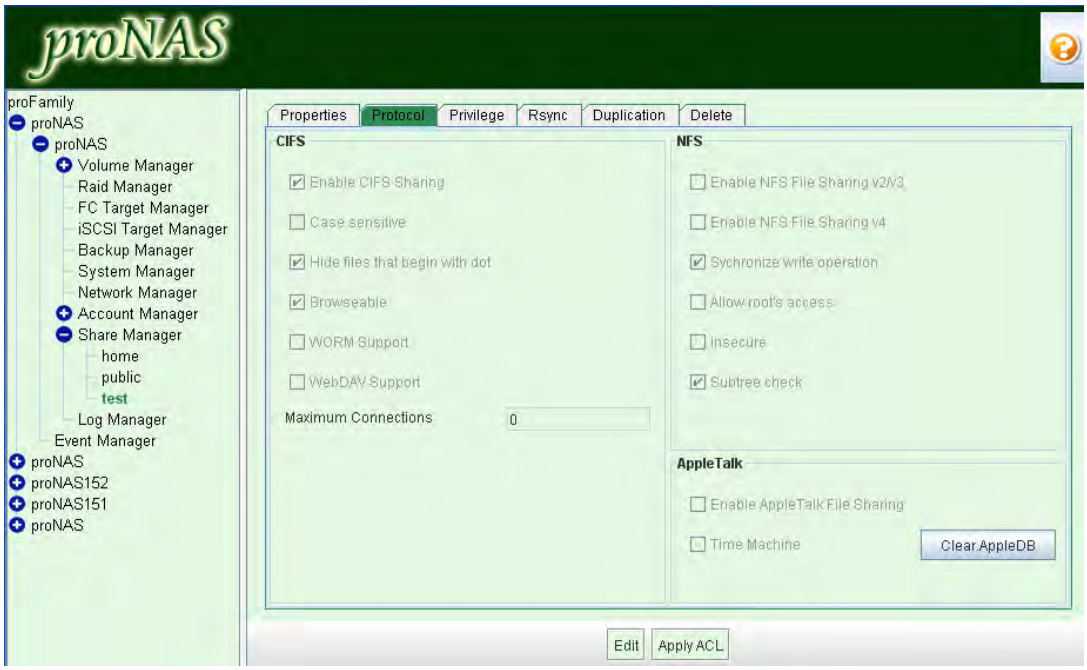
14. Done. The Time Machine will automatically backup to the designated NAS share folder.

5.6.3.5 How to Use WORM

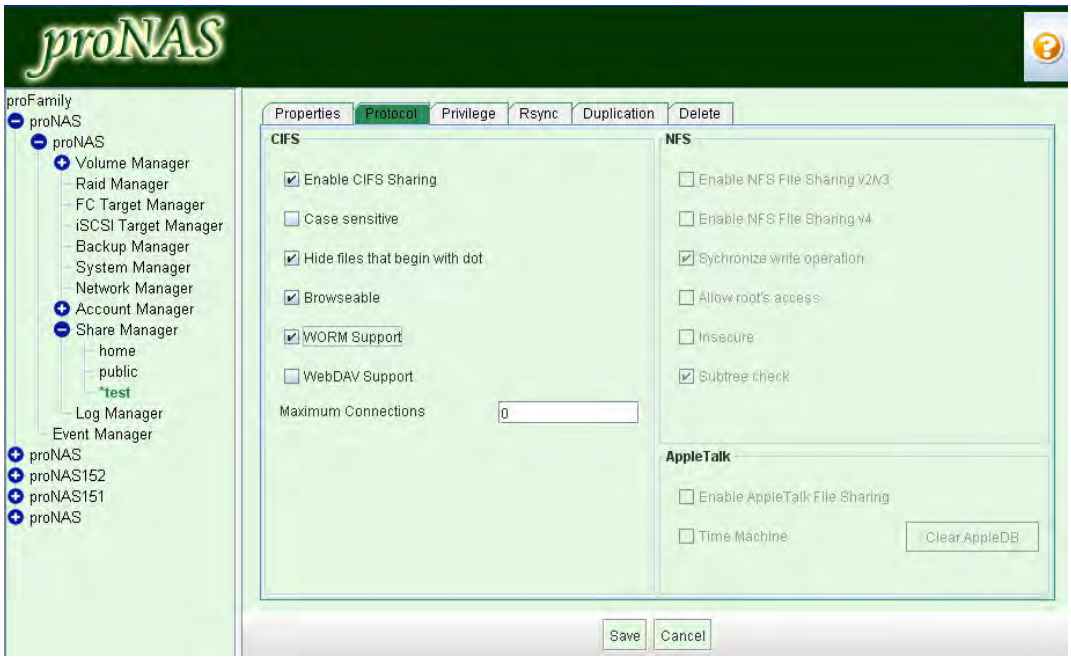
WORM (Write Once, Read Many) allows data to be written once to a share folder, and prevents data to be erased. After data is written, it will become read-only.

Steps:

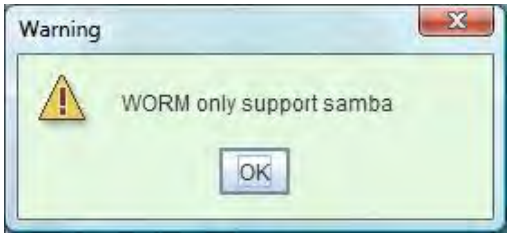
1. Create a share folder under Share Manager. Then select Protocol tab. Click “Edit”.



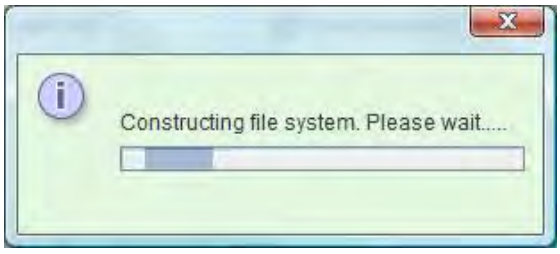
2. Tick “WORM Support”.



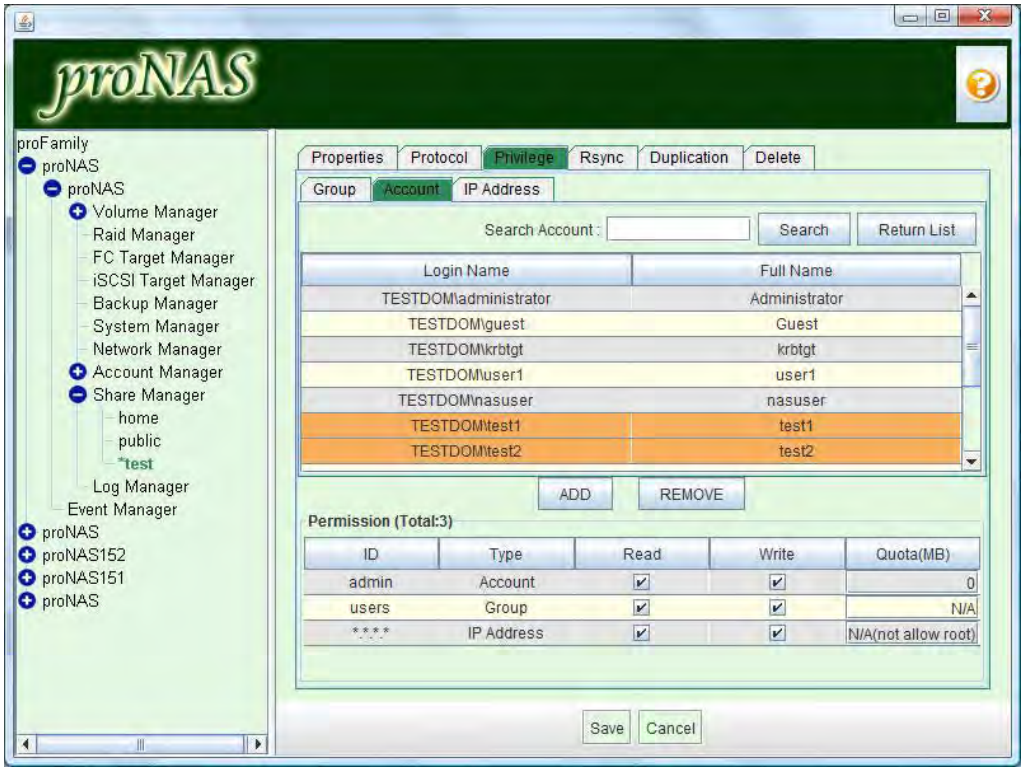
3. A warning message will be displayed. Click “OK”.



4. Click “Save” when done. The share folder setting will be updated.



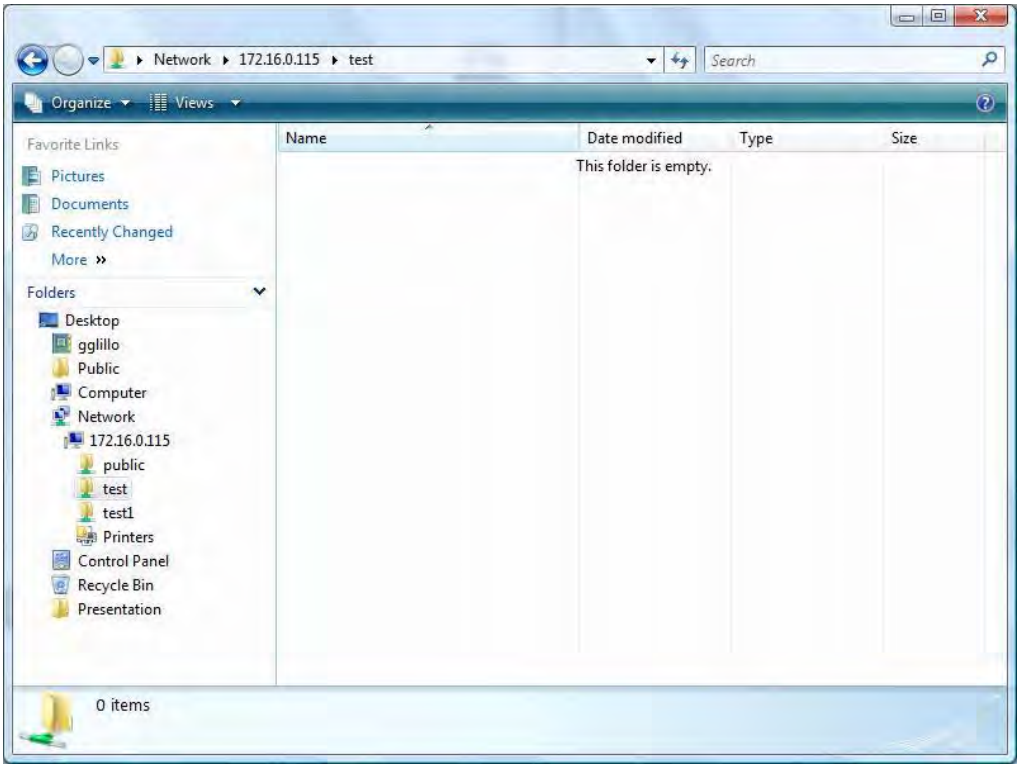
5. Select Privilege tab. Select Account tab to add share folder permission for domain accounts.



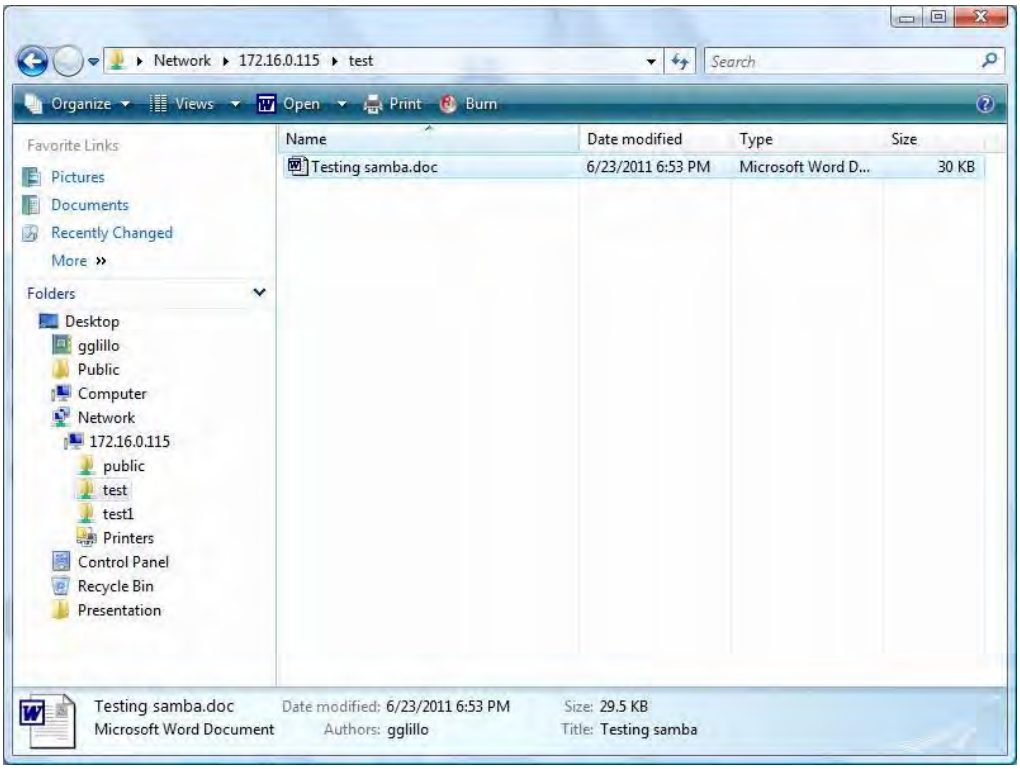
6. Add the domain accounts to the permission list. Click “Save” when done.

7. Login NAS share folder using a valid user name and password (account with permission to the share folder).

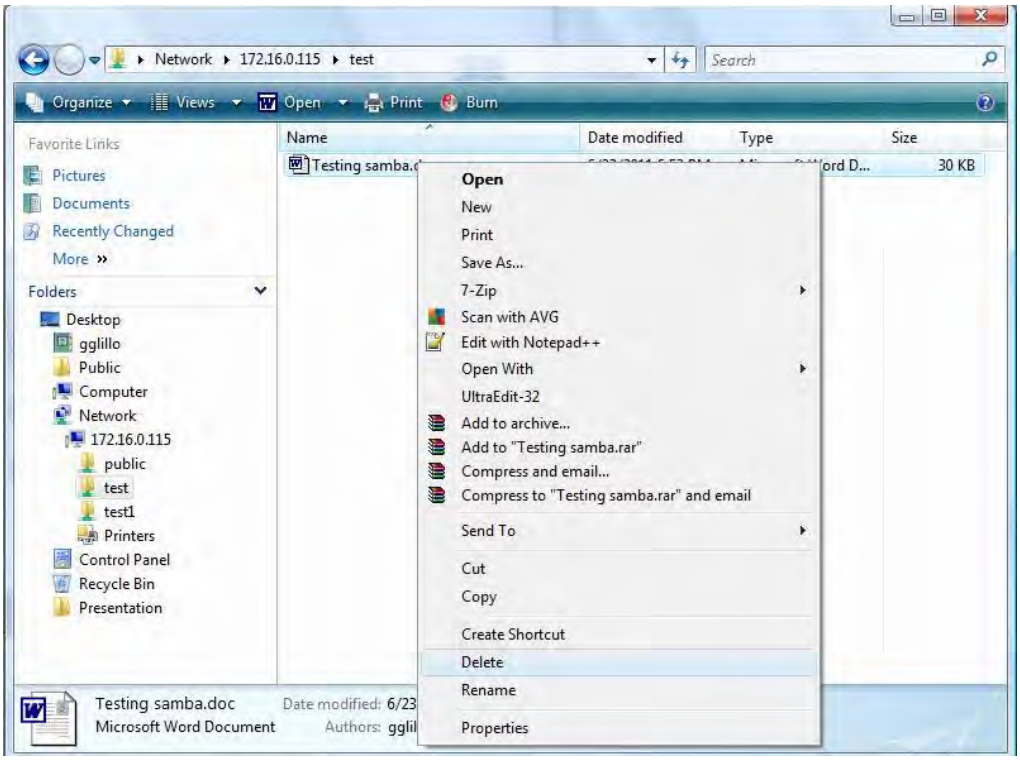
8. Open the share folder.



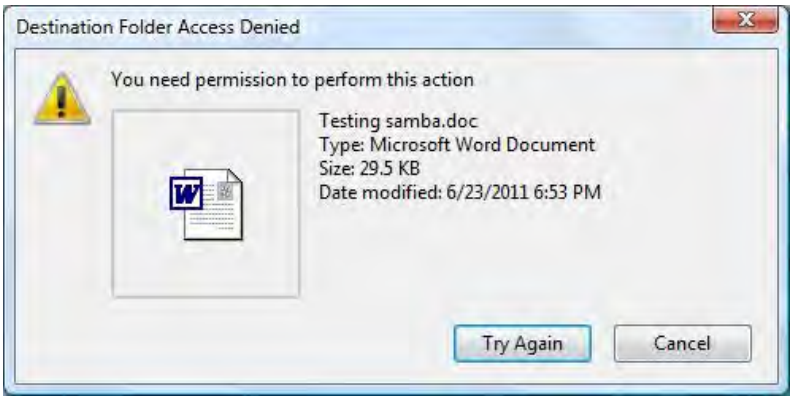
9. Copy a file.



10. Right-click the file and select “Delete” from the pop-up menu.



11. Notice that the file cannot be deleted. It will be accessible as read-only.

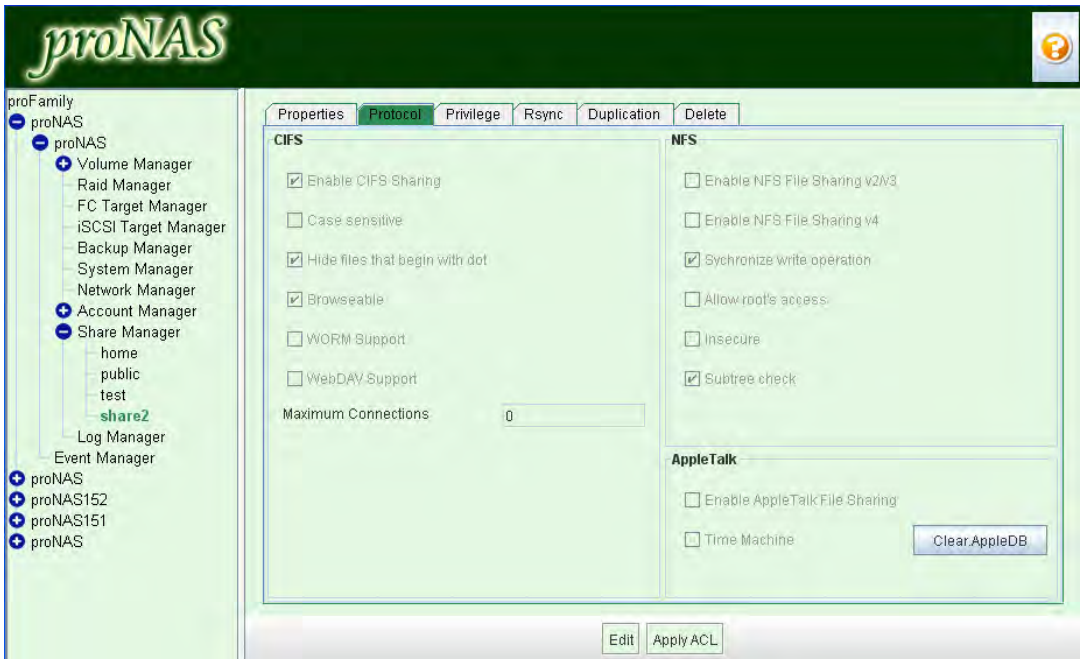


5.6.3.6 How to Use WebDAV

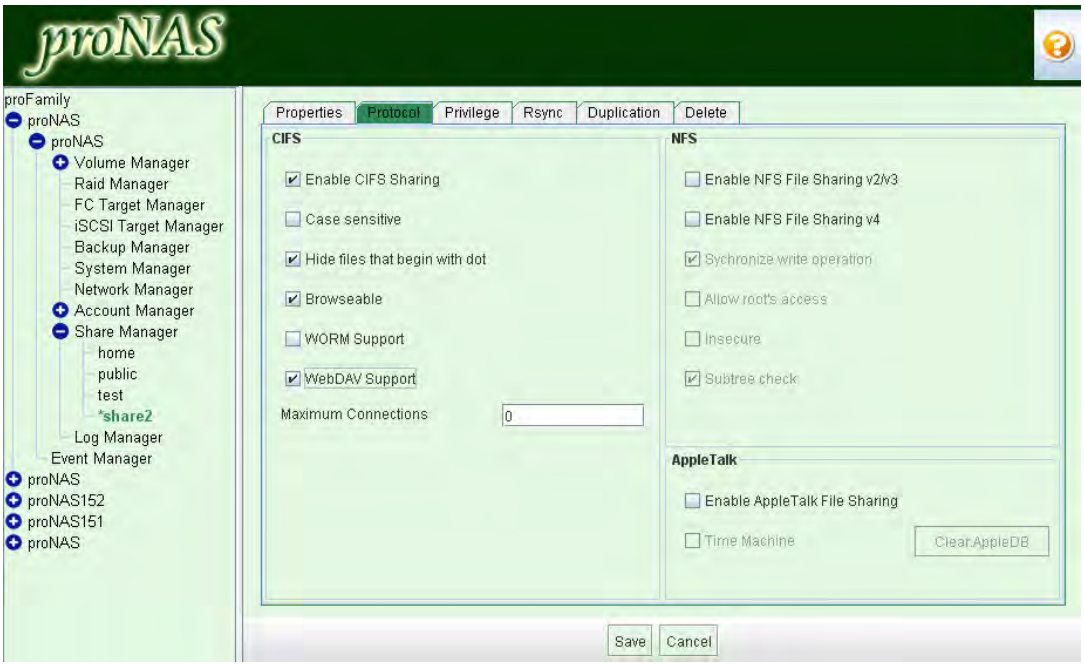
WebDAV allows users to access their data through the web using HTTP protocol.

Steps:

1. Create a share folder under Share Manager. Then select Protocol tab. Click “Edit”.

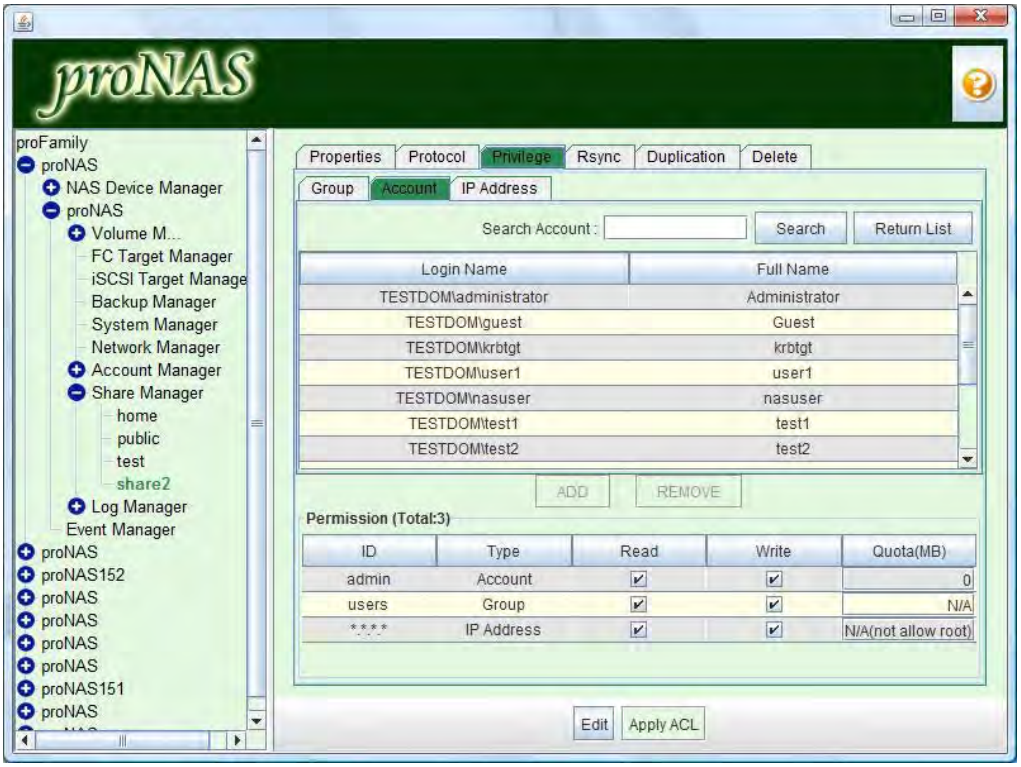


2. Tick “WebDAV Support”.



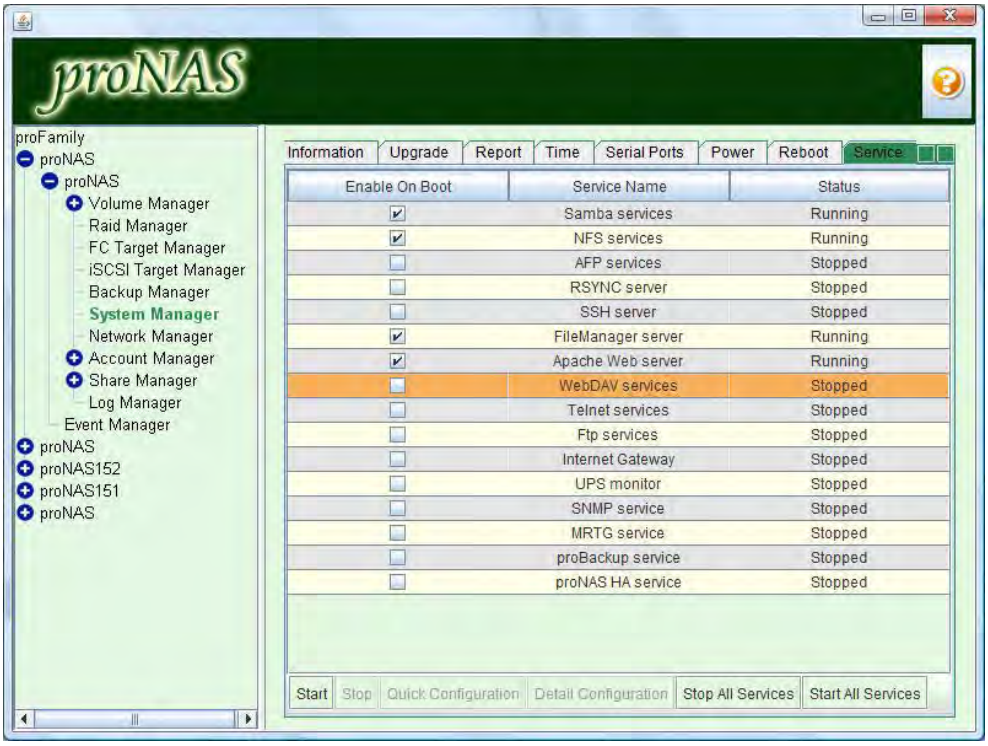
3. A warning message will be displayed. Click “OK”.

4. Select Privilege tab. Select domain users that will be allowed access to the share folder, and add to the Permission list.

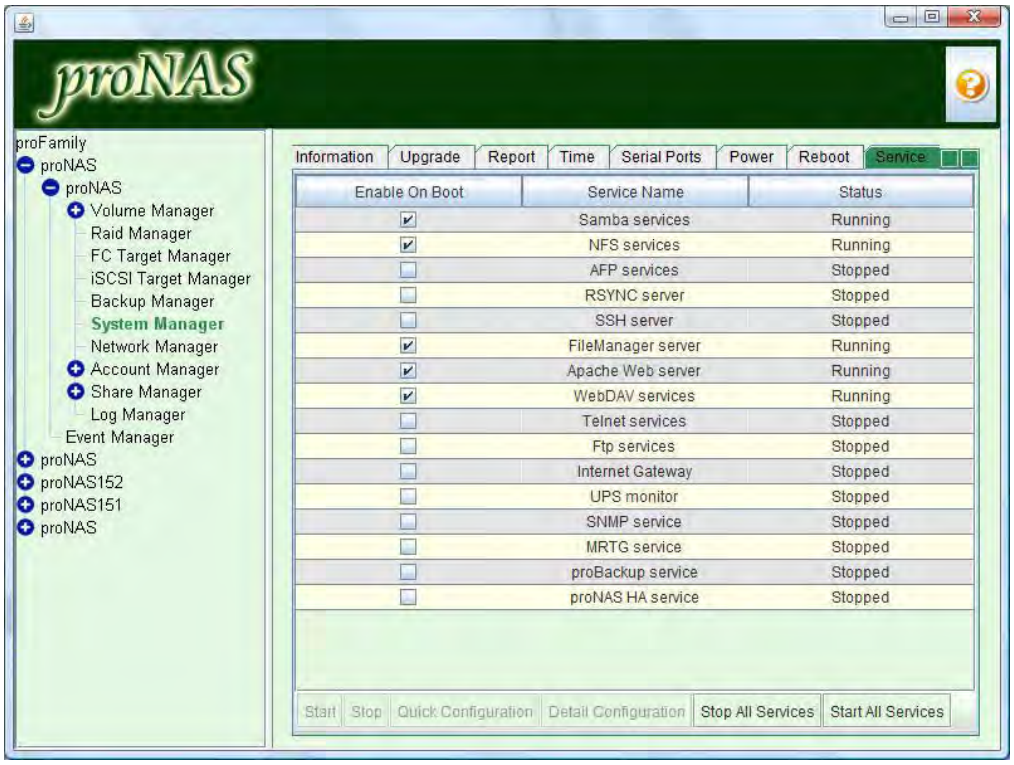


5. Click “Save” when done.

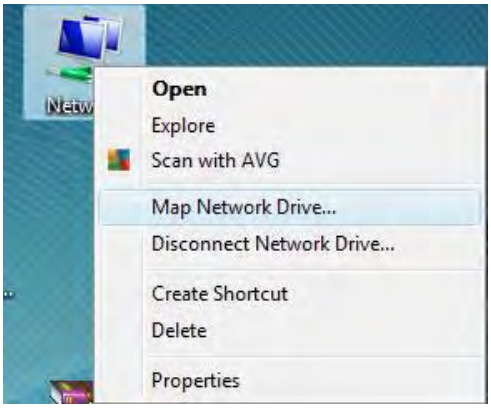
6. Select System Manager, Service tab. Select “WebDAV services” and click “Start’ to enable WebDAV service.



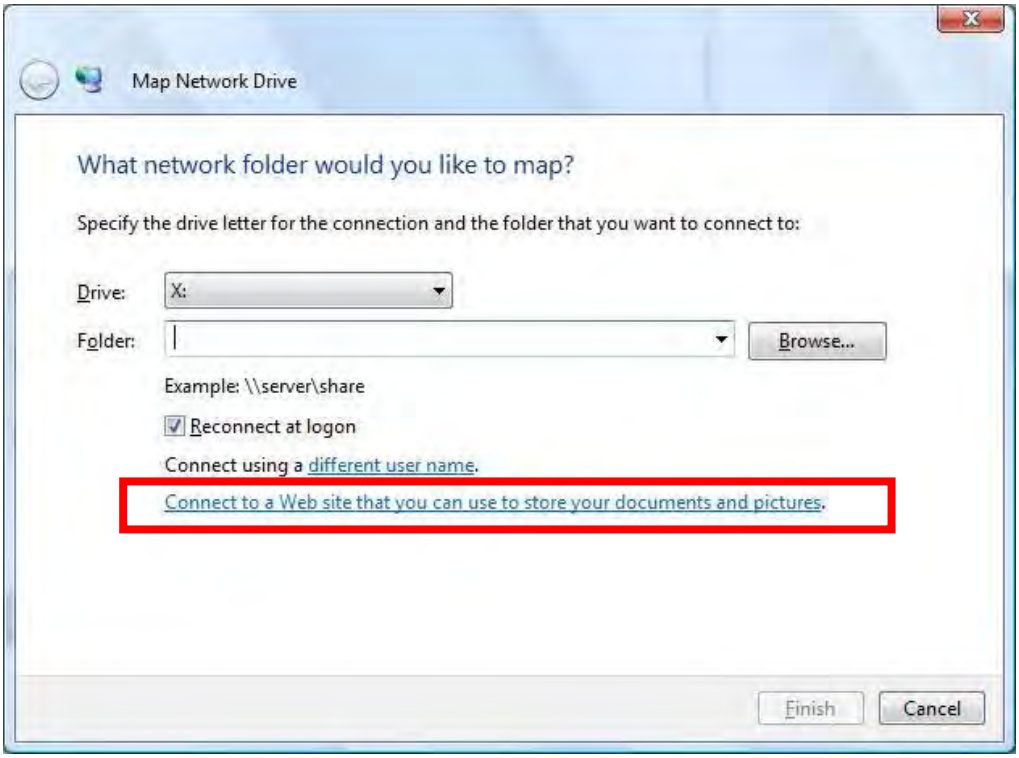
7. The WebDAV service will be running. You can also select “Enable On Boot” option.



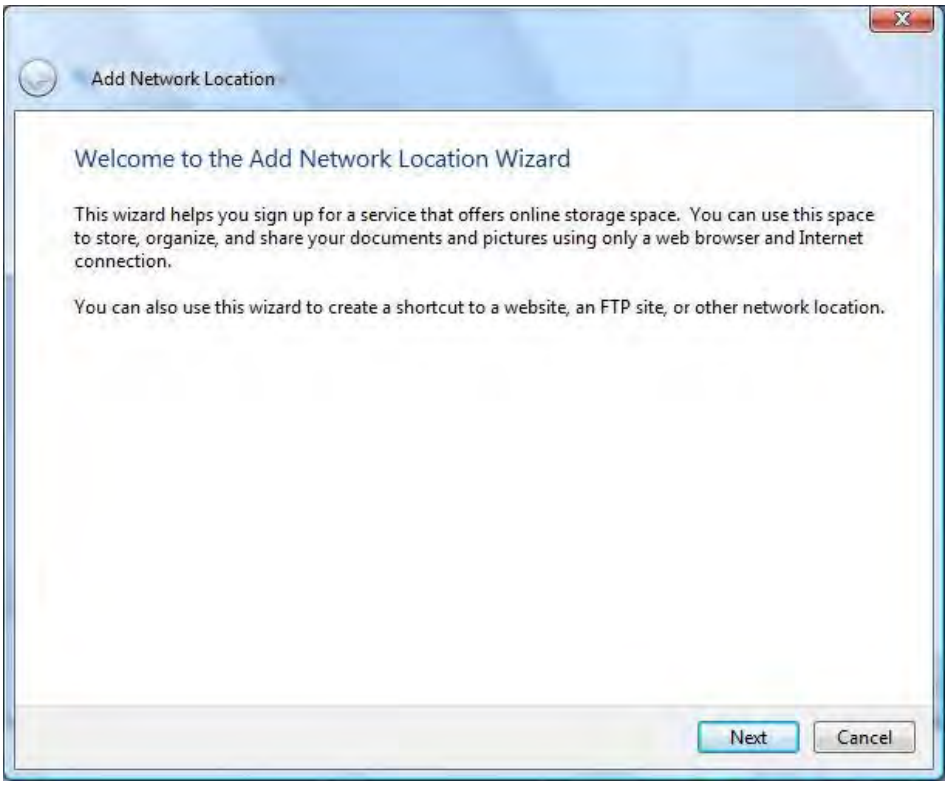
8. In a Windows PC, right click Network icon to map network drive. From the pop-up menu, select “Map Network Drive…”.



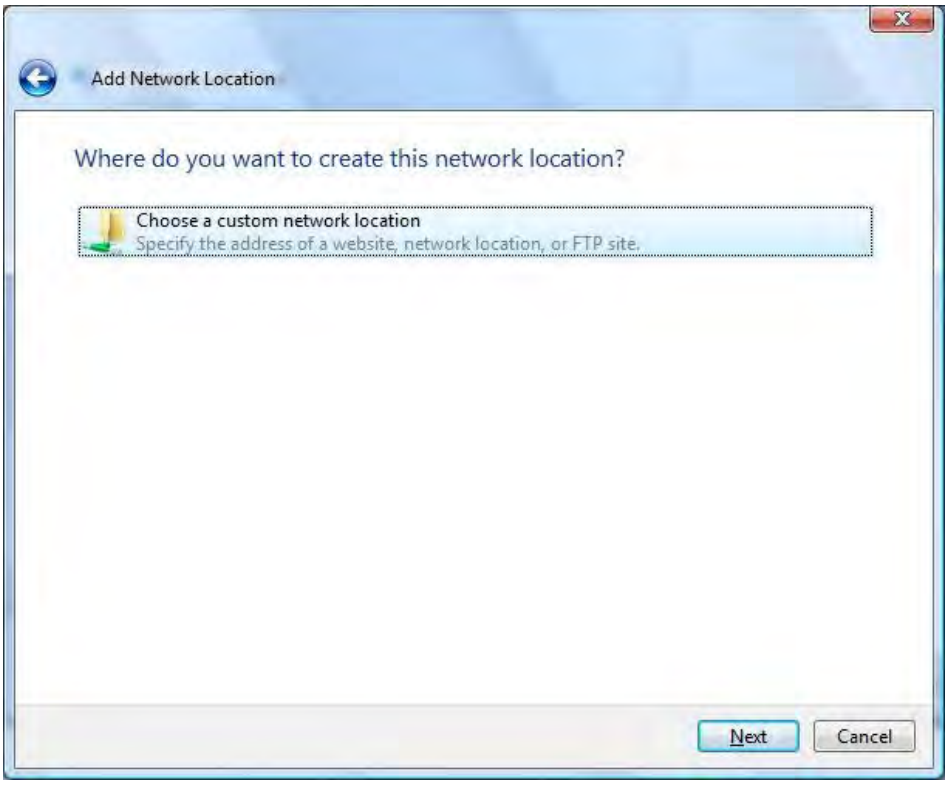
9. Click “Connect to a Web site that you can use to store your documents and pictures.”


Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
X:
Folder:
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

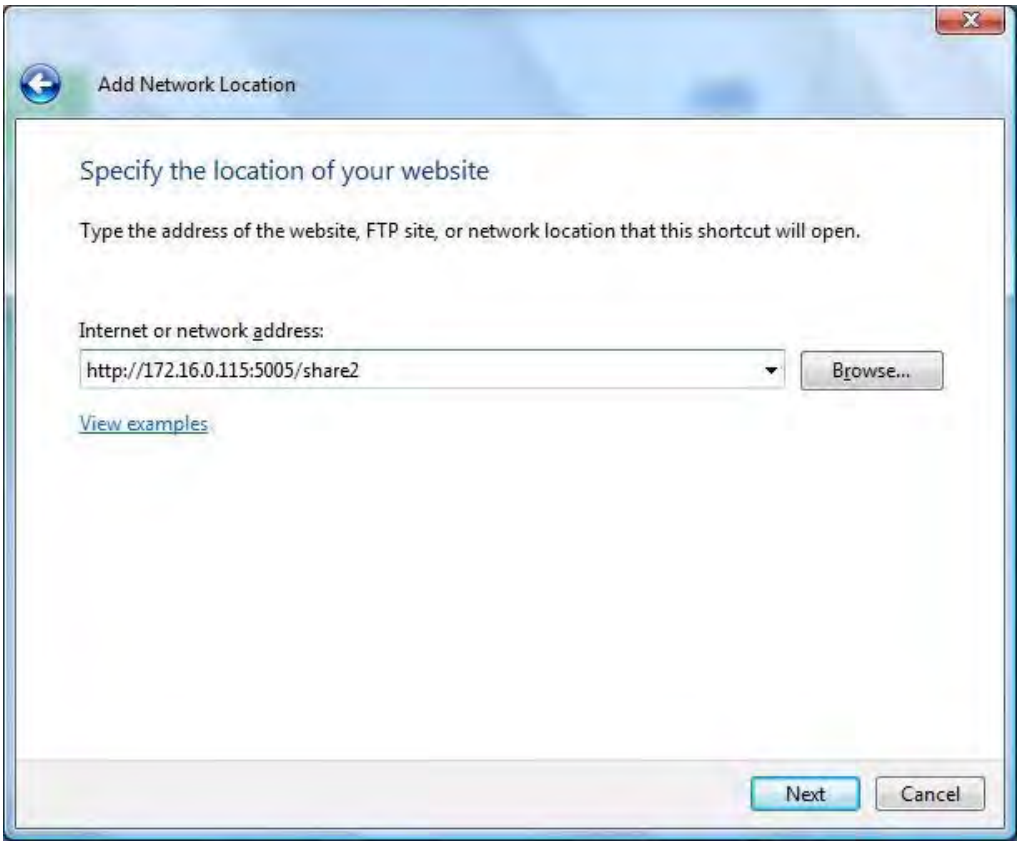
10. In Add Network Location, click “Next”.


Add Network Location
Welcome to the Add Network Location Wizard
This wizard helps you sign up for a service that offers online storage space. You can use this space to store, organize, and share your documents and pictures using only a web browser and Internet connection.
You can also use this wizard to create a shortcut to a website, an FTP site, or other network location.
Next
Cancel

11. Click “Next”.


Add Network Location
Where do you want to create this network location?
Choose a custom network location
Specify the address of a website, network location, or FTP site.
Next
Cancel

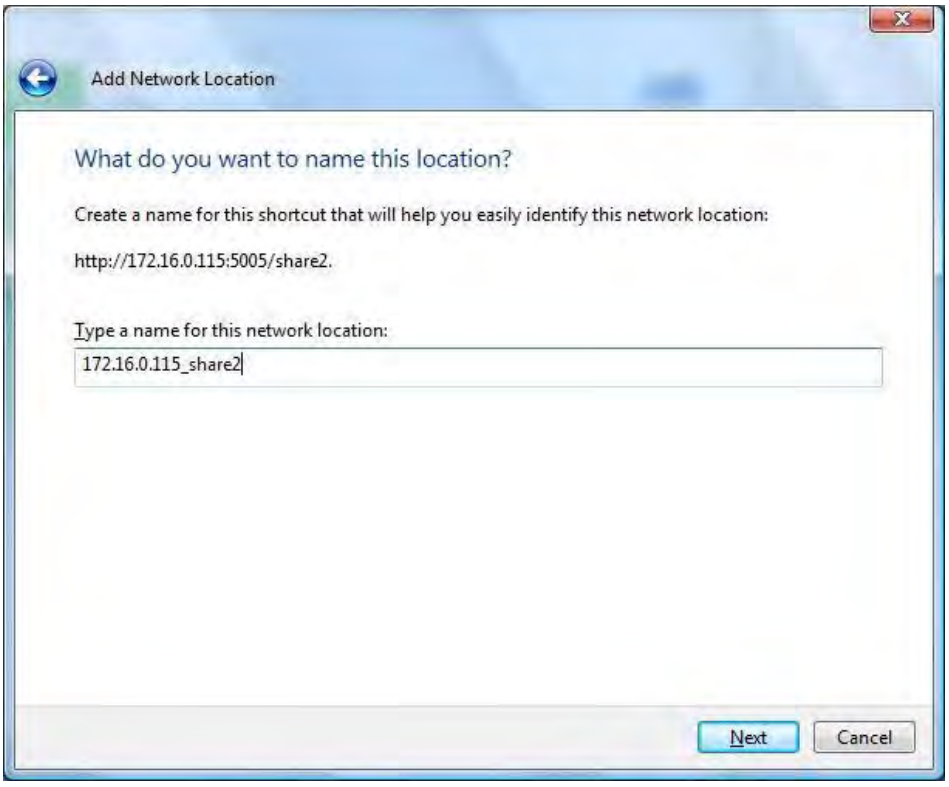
12. In “Internet or network address:” box, enter internet address of the NAS using the NAS IP and port 5005, and then the share folder name. For example: **http://172.16.0.111:5005/share2** Click “Next” when done.



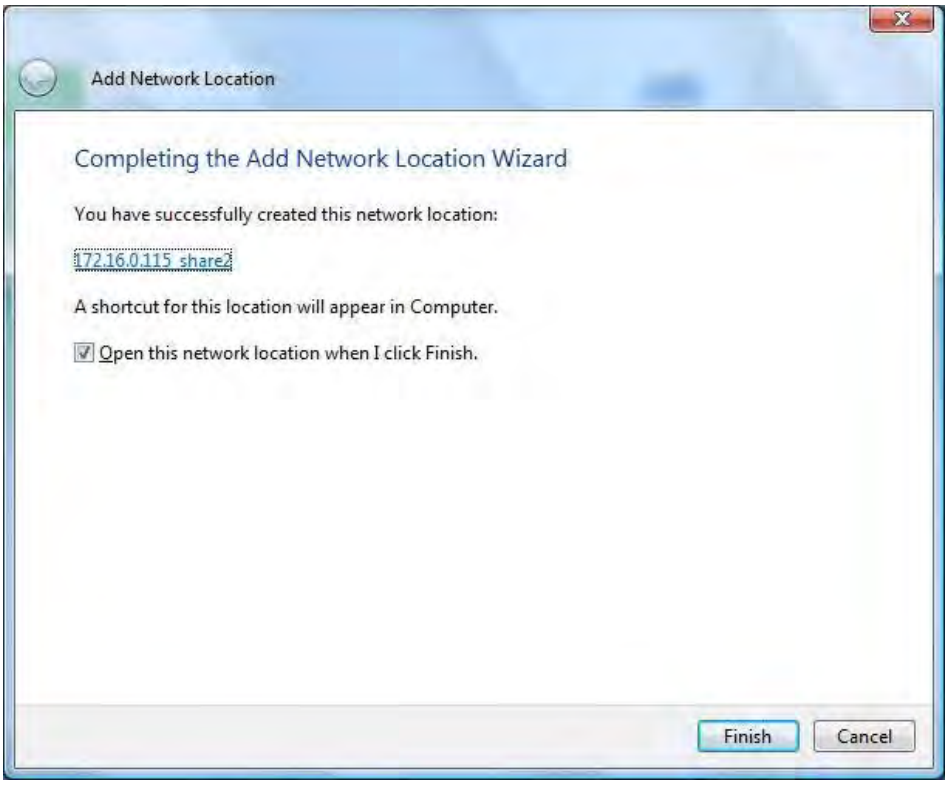
13. In the Login screen, enter the user name and password. Note that the user name must be an account that was added to the share folder permission in Step 5.

Connect to 172.16.0.115
The server 172.16.0.115 at Login requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
TESTDOM\test1
Password:
Remember my password
OK
Cancel

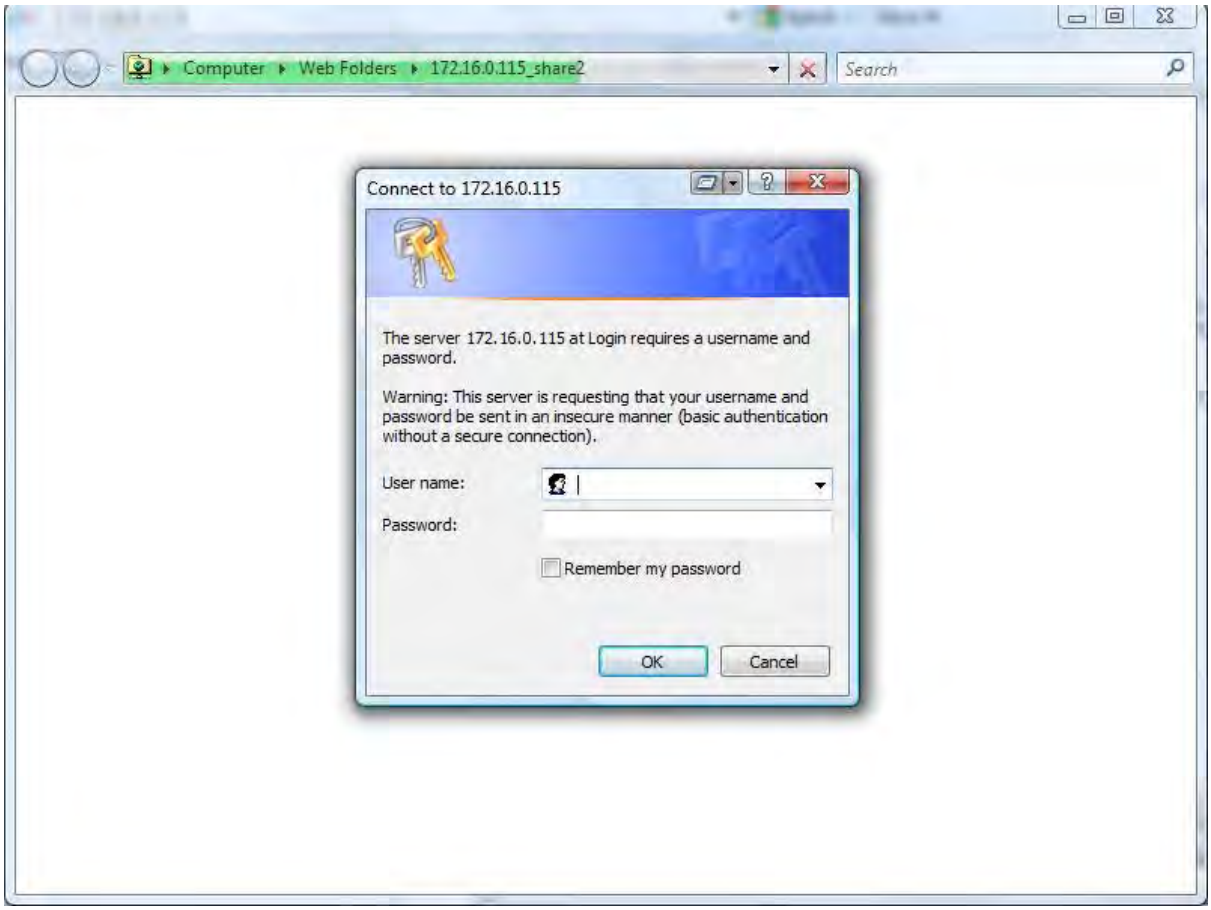
14. Enter a name for the network location. Click “Next”.


Add Network Location
What do you want to name this location?
Create a name for this shortcut that will help you easily identify this network location:
http://172.16.0.115:5005/share2.
Type a name for this network location:
172.16.0.115_share2
Next
Cancel

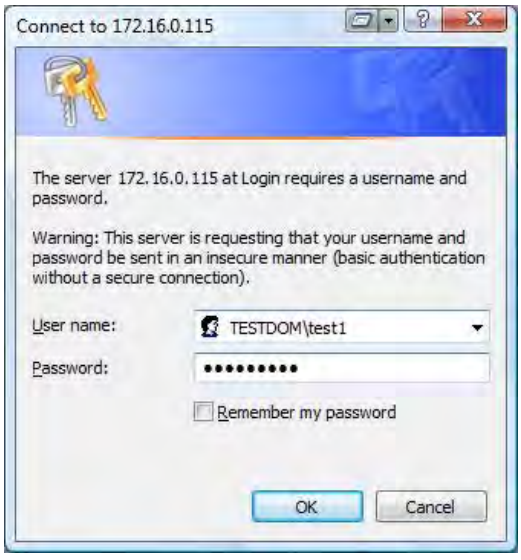
15. Click “Finish”.


Add Network Location
Completing the Add Network Location Wizard
You have successfully created this network location:
172.16.0.115_share2
A shortcut for this location will appear in Computer.
Open this network location when I click Finish.
Finish
Cancel

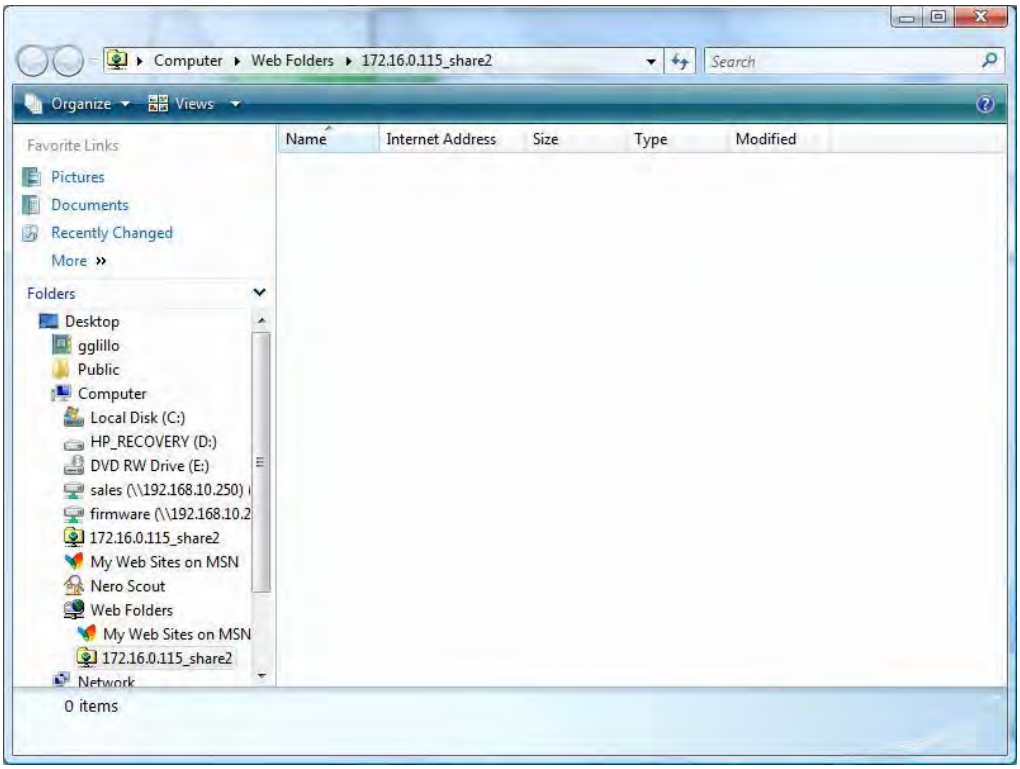
16. To login to the web folder, enter a valid user name and password.


Computer
Web Folders
172.16.0.115_share2
Search
Connect to 172.16.0.115
The server 172.16.0.115 at Login requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

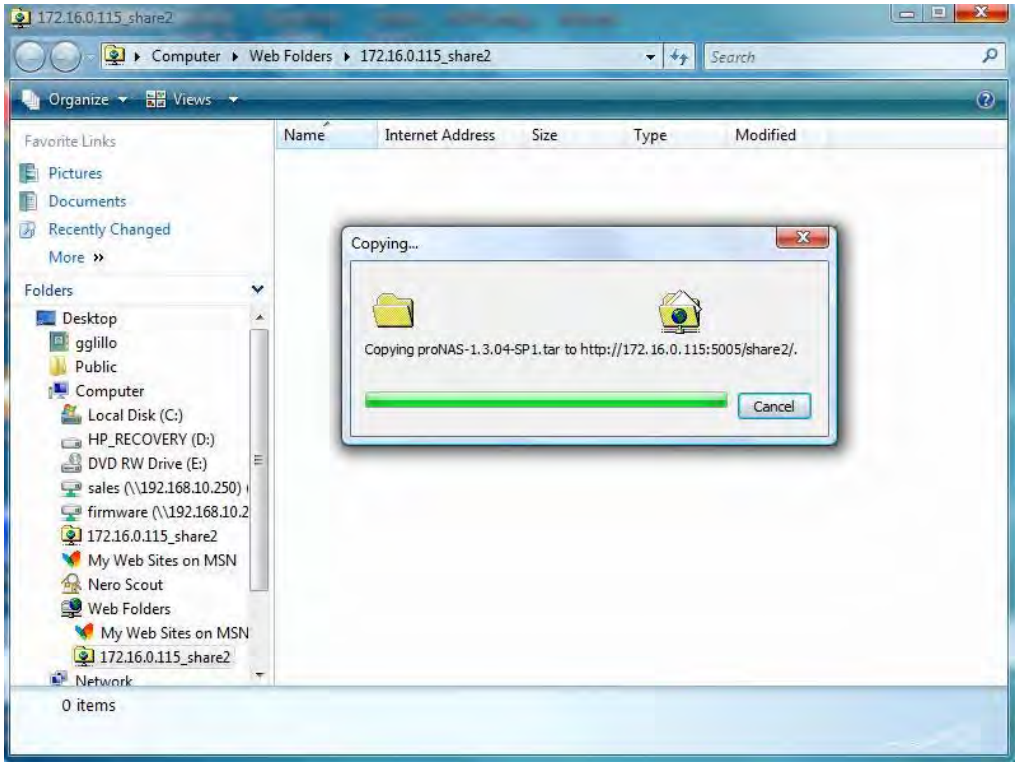
17. After entering user name and password, click “OK”.


Connect to 172.16.0.115
The server 172.16.0.115 at Login requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
TESTDOM\test1
Password:
Remember my password
OK
Cancel

18. After login, you can start to use your web folder.



19. You can copy file(s) to the web folder.



5.6.4 Privilege (Permission Setting)

Using Privilege tab, administrator can set the ACL (Access Control List) for share folder either by Group, Account, or IP Address.

NOTE: Only up to 64 entries in the Permission list is allowed for each share folder. If it is needed to have more than 64 entries, a workaround is to create a group whose members are the user accounts which will have same permission to the share folder. Then assign permission only to the group, instead of assigning permission to each individual user account.

5.6.4.1 Group

You can assign specific group read or read/write permission for certain share folder. Choose the group and press "ADD" button. The group will displayed in the permission list, and check "Read" or "Write" or check both and press "Save". If you would like to remove the group with ACL setting to certain share folder, select the group name and press "REMOVE" button.

Sample Steps to Assign Group Account Permission to Share:

1. Select Share Manager. Select the share name where account will be given permission, and click Privilege tab.
2. Click “Edit”. Select Group tab.
3. Select the group account that will be given permission and click “ADD”.

NOTE: When group account name is selected, it will be highlighted. If you want to select more than one group account at the same time, press “Shift” key then click the groups you want to add to Permission list.

4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).

5. Click Save.

5.6.4.2 Account

You can assign specific account user read or read/write permission for certain share folder. When you set the account with ACL, it may be necessary to remove the users group from the permission list in order to prevent access of other members of “users” group to the share. Choose the account and press "ADD" button, and the account will be displayed in the permission list. Check "Read" or "Write" or check both and click the "Save" button.

NOTE: Newly added users or groups may have no permissions on the existing files or sub-folders under the share until "Apply ACL" button is executed in that share.

Setting the amount of share quota to a specific user account

In the "Quota(MB)" field, you can input the quota of an account which is granted permission to the share. After clicking “Edit”, input the quota size in Quota(MB) field and then press the "Enter" key. To remove the quota limit, set the Quota(MB) to 0 then press "Enter" key. Click “Save” when done.

NOTE: The account quota set in Privilege section of Share folder setting applies only to the share folder itself. Other share folders can be set with different user account quota. Also, this quota is different from the user account’s quota in his “home” folder.

Sample Steps to Assign User Account Permission to Share:

1. Select Share Manager. Select the share name where account will be giver permission, and click Privilege tab.
2. Click “Edit”. Select Account tab.
3. Select the account name that will be given permission and click “ADD”.

NOTE: When account name is selected, it will be highlighted. If you want to select more than one account at the same time, press “Shift” key then click the accounts you want to add to Permission list.

4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).
5. Click Save.

5.6.4.3 IP Address

This option allows you to set a certain range of hosts (IP) to have an access into proNAS. By default, the IP address is set to *.*.*.* which means that it will accept connections from any host. If set to 192.168.100.*, this will only allow connections from your private network 192.168.100 and all other connections will be refused.

NOTE: Not all ACL permission settings may be applicable to all share protocols. If you set NFS protocol, it can support all ACL setting such as Read-only IP or Read/Write IP. If you set CIFS protocol, Read-only IP address is not honored, which means the IP address or addresses included in the ACL as Read-only IP will still have Read/Write permission when connected via CIFS. AppleTalk/AFP also does not honor Read-only IP same as CIFS.

Sample Steps to Limit Share Connections to Selected IP Range:

1. Select Share Manager. Select the share name where account will be given permission, and click Privilege tab.
2. Click “Edit”. Select IP Address tab.

NOTE: By default, all IP addresses (*.*.*.*) have Read/Write access to the NAS. If you restrict NAS connections from specific IP range, only the selected IP range can access the NAS share. Group Permission or User Account Permission is still needed to be assigned in order for users to gain access to the share folder.

3. To remove *.*.*.*, select “*.*.*.*” from Permission list and click “REMOVE”.
4. To add an IP range, enter the IP range (e.g.: 192.168.1.*) in the “IP Address” box, check the “Write” box to assign Read/Write access if necessary, and click “ADD”.
5. Click “Save” when done.

Permissions:

This section lists the permissions that you can assign for each user, group, or IP address. When you create a share, the default owner which is the "admin" will be granted full control. The same is also true for "users" group and the "*.*.*.*" for IP address.

Listed below are the share permissions defined in proNAS:

Read Only			**Read+Write**		
	Allow	Deny		Allow	Deny
Access share, sub-folder	☑		Access share, sub-folder	☑	
Read	☑		Read	☑	
Write		☑	Write	☑	
Edit/Modify		☑	Edit/Modify	☑	
Delete		☑	Delete	☑	
Rename		☑	Rename	☑	

5.6.5 Rsync

Rsync copies files either to or from a remote host, or locally on the current host. It is also a utility that provides fast incremental file transfer. proNAS Rsync implementation can be set either in server mode or client mode. Server mode means that proNAS can accept incoming Rsync connections, where as in client mode, proNAS is the one who initiates the synchronization. To use as a server mode, you must start the "RSYNC server" first. Go to System Manager -> Service tab, highlight "RSYNC server" then click the "Start" button.

Some of the additional features of Rsync are:

- Support for copying links, devices, owners, groups, and permissions.
- Pipelining of file transfers to minimize latency costs
- Support for anonymous or authenticated Rsync daemons

Server Mode:

When proNAS system is in Server Mode, the Rsync clients can connect either within a local transfer, via a remote shell or via a network socket.

- Enable - When checked, proNAS is set as a Rsync server.
- Read only - When checked, all files within this share will be read only to any Rsync client.
- Anonymous - When checked, anonymous connections will be accepted.
- Maximum Connections - This specifies the maximum number of Rsync client that can connect to this share at a certain time.
- Edit accounts - You may edit and existing account, or add/delete a user. These accounts are the accounts that need to be supplied by the Rsync clients when connecting to this server.

Client Mode:

The proNAS system will initiate the synchronization and contact an Rsync server. There are two different ways for Rsync to contact a remote system: using SSH as a remote-shell program as the transport or contacting an Rsync daemon directly via TCP.

- IP Address - This specifies the IP address of the remote Rsync server.
- Remote Path - This specifies the share on the remote Rsync server.
- Account - The valid account name that will be required by the Rsync server for authentication.
- Password - The account's password.
- Mode - Either to download files from the Rsync server or to upload files into the Rsync server.
- SSH - When checked, SSH service will provide the secure tunnel between an Rsync client and an Rsync server.
- Rsync Options - These are the lists of options used during Rsync file transfer

Here is a short summary of the available options. Please refer to the detailed description below for a complete description. Some options only have a long variant.

-r, --recursive	recurse into directories
-v, --verbose	increase verbosity. This option increases the amount of information your are given during the transfer
-l, --links	copy symlinks as symlinks
-p, --perms	preserve permissions. This option causes the receiving Rsync to set the destination permissions to be the same as the source permissions.
-o, --owner	preserve owner (super-user only). This option causes Rsync to set the owner of the destination file to be the same as the source file
-g, --group	preserve group. This option causes Rsync to set the group of the destination file to be the same as the source file.
--ignore-existing	Ignore files that already exist on the receiver. This tells Rsync to skip updating files that already exist on the destination.
-b, --backup	With this option, preexisting destination files are renamed as each file is transferred or deleted. You can control where the backup file goes and what (if any) suffix gets appended using the --backup-dir and --suffix options
--backup-dir=dir	In combination with the --backup option, this tells Rsync to store all backups in the specified directory. This is very useful for incremental backups. You can additionally specify a backup suffix using the --suffix option (otherwise the files backed up in the specified directory will keep their original filenames).
--suffix=SUFFIX	This option allows you to override the default backup suffix used with the --backup (-b) option. The default suffix is a ~ if no --backup-dir is specified, otherwise it is an empty string.
-D, --devices	preserve device files
--specials	preserve special files
-t, --times	preserve times
-S, --sparse	handle sparse files efficiently
-z, --compress	Compresses file data during the transfer. This option is useful in slow links.
-a, --archive	This is equivalent to -rlptgoD. It is a quick way of saying you want recursion and want to preserve almost everything (with -H being a notable omission).
-E, --executability	This option causes Rsync to preserve the executability (or non-executability) of regular files when --perms is not enabled.
-h, --human-readable	Output numbers in a human-readable format.
--stats	Give some file-transfer stats.
--delete	Delete files that don't exist on the sender.
--log-file-format=FORMAT	Output filenames using the specified format.
--log-file=FILE	Output filenames using the specified file.

--bwlimit=KB/S Limit I/O bandwidth; KBytes per second.

-n, --dry-run This tells Rsync to not do any file transfer; instead it will just report the actions it would have taken.

--timeout=SECS Sets the maximum I/O timeout in seconds. If no data is transferred for the specified time then Rsync will exit. The default is 0, which means no timeout.

There are lot more useful options that are not included in this list. It may vary depending on your usage, for more information on Rsync, please visit http://samba.org/rsync/.

After completing the above settings, you can run the Rsync client task immediately by clicking the "Execute" button.

Rsync Schedule

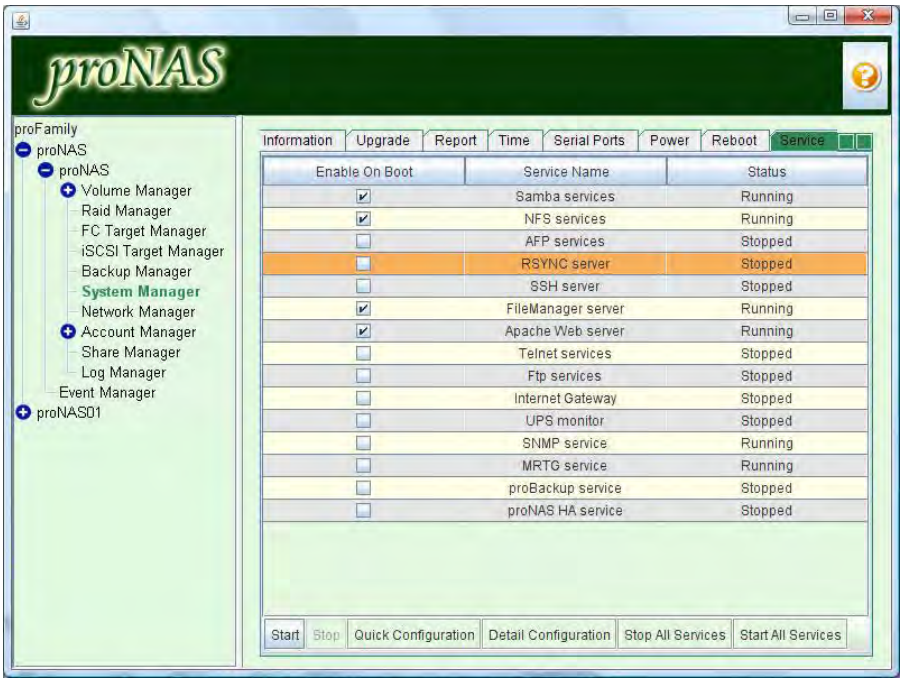
You can automate the Rsync client tasks simply by running it thru schedule. Please select which day(s) to run, the time of the day or if by interval, select a time then set the starting/ending time and then enable the schedule by clicking on the "Enable Scheduled" button.

5.6.5.1 How to Setup Rsync

In this example, a NAS is setup as Rsync server and will be the destination for Rsync backup. Another NAS is setup as Rsync client and will be the source of Rsync files. Data will be uploaded from Rsync client (source) to Rsync server (destination).
Rsync server has host name “proNAS-B” and IP address 172.16.0.12, while Rsync client has host name “proNAS1303” and IP address 172.16.0.11.

A. How to Setup the NAS as Rsync Server

1. Login to proNAS GUI of the NAS that will be designated as Rsync server. In System Manager → Service, start “Rsync server”.

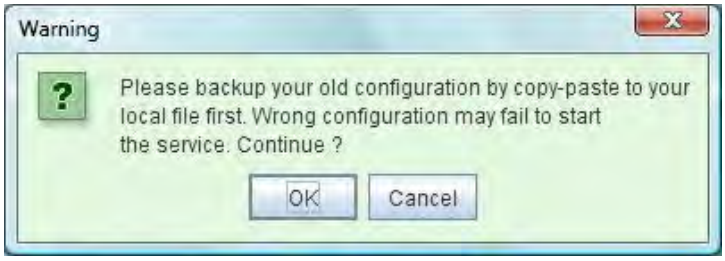


2. In Share Manager, select the share folder that will be used as Rsync Server share folder. Click “Edit” and select the option “Server Mode”. Select (tick) the “Enable” option in Server Mode screen.

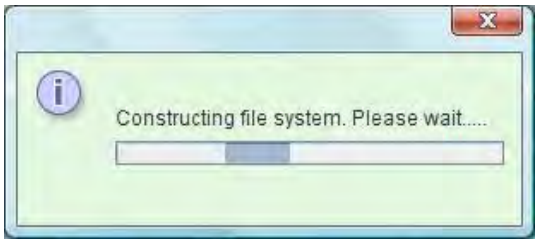
3. Click the “Edit Accounts” button and input a username and password entry, for example “**admin:proware**”. Click “Save” when done.

NOTE: The username and password entry here is used in Client Mode Setup (part B, step #2) Account and Password.

4. A warning message will be displayed. Click “OK” to continue.


Warning
Please backup your old configuration by copy-paste to your local file first. Wrong configuration may fail to start the service. Continue ?
OK
Cancel

5. Click “Save” to save settings. The Rsync server settings will be saved.



B. How to Setup the NAS as Rsync Client:

1. Login to proNAS GUI of the NAS that will be designated as Rsync client. Select the share folder the will be used as data source and click the Rsync tab.

2. Click “Edit” button. Setup the Rsync client options, such as IP Address, Remote Path, Account, Password, Mode, and Rsync options if necessary.

NOTE: Only one share folder can be selected and used for Rsync, since the remote path is also a single share folder.

Sample Setting:

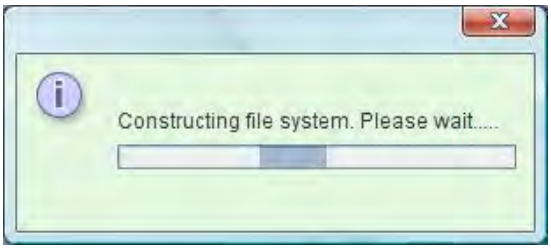
IP:	**172.16.0.12**
Remote Path:	**dest**
Account:	**admin**
Password:	**proware**
Mode:	**Upload**
Rsync Options:	**-rvlHpogDtS –progress**

NOTE: The Account and Password entry here should be a valid username:password combination entered in Server Mode (part A, step #3) Edit Accounts.

Summary of Rsync default options:

-r, --recursive	Recurse into directories
-v, --verbose	Increase verbosity. This option increases the amount of information given during the transfer
-l, --links	Copy symlinks as symlinks
H, --hard-links	Preserve hard links
-p, --perms	Preserve permissions. This option causes the receiving Rsync to set the destination permissions to be the same as the source permissions.
-o, --owner	Preserve owner (super-user only). This option causes Rsync to set the owner of the destination file to be the same as the source file
-g, --group	Preserve group. This option causes Rsync to set the group of the destination file to be the same as the source file.
-D, --devices	Preserve device files
-t, --times	Preserve times
-S, --sparse	handle sparse files efficiently
--progress	Show progress during transfer (shown in the Rsync log)

3. Click “Save”. The Rsync client setup will be saved.

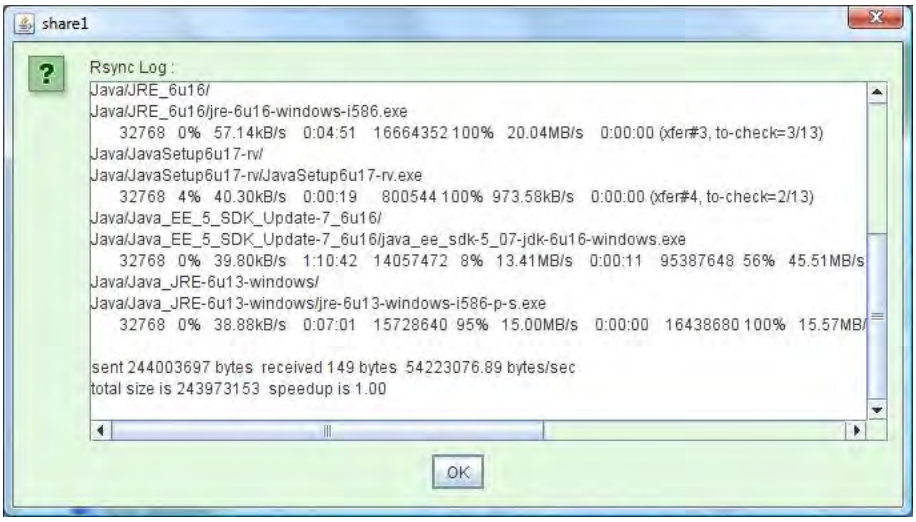


4. To immediately execute Rsync to upload data from Rsync client (source share) to Rsync server (destination share) click “Execute”. When a Confirmation message appears, click “Yes” to proceed.

5. The Rsync process will be started. The Rsync status (x/y Completed) will be shown.

NOTE: The Rsync process can take a while if there are many files to be updated / uploaded or downloaded.

6. To view the Rsync log, click “Get Log” button. The log will be shown. Click “OK” to close the Rsync log.


share1
Rsync Log :
Java/JRE_6u16/
Java/JRE_6u16/jre-6u16-windows-i586.exe
32768 0% 57.14kB/s 0:04:51 16664352 100% 20.04MB/s 0:00:00 (xfer#3, to-check=3/13)
Java/JavaSetup6u17-rv/
Java/JavaSetup6u17-rv/JavaSetup6u17-rv.exe
32768 4% 40.30kB/s 0:00:19 800544 100% 973.58kB/s 0:00:00 (xfer#4, to-check=2/13)
Java/Java_EE_5_SDK_Update-7_6u16/
Java/Java_EE_5_SDK_Update-7_6u16/java_ee_sdk-5_07-jdk-6u16-windows.exe
32768 0% 39.80kB/s 1:10:42 14057472 8% 13.41MB/s 0:00:11 95387648 56% 45.51MB/s
Java/Java_JRE-6u13-windows/
Java/Java_JRE-6u13-windows/jre-6u13-windows-i586-p-s.exe
32768 0% 38.88kB/s 0:07:01 15728640 95% 15.00MB/s 0:00:00 16438680 100% 15.57MB/
sent 244003697 bytes received 149 bytes 54223076.89 bytes/sec
total size is 243973153 speedup is 1.00
OK

7. Rsync can also be run on schedule. Setup the schedule in Schedule tab on Client Mode.

5.6.6 Duplication

Duplication is a file level snapshot utility for making backups of your local filesystem. Using Duplication, it is possible to take incremental snapshots of your filesystem at different points in time. Duplication creates the illusion of having a multiple full backups by using hard links, while only taking up the space of one full backup plus differences. This saves much more disk space than one might image. The duplication files will be directed to a share which can be accessed via share protocols or by Telnet service.

Duplication can be invoked manually or by schedule.
Select the share folder in Share Manager then click “Edit” button.

Creating Duplication by Schedule

To create duplication by schedule, first set the number of total duplication that will be created, specify which day to be run, set the time task whether by interval or once in a specific time of day, set the destination path and then click “Save” button. Enable the schedule by clicking on the "Enable Scheduled" button. To disable the scheduled duplication, just click on the "Disable Scheduled" button.

The Duplication tab information is shown below.

Execute Day:	Specifies whether the scheduled task is to run on this day.
Execute Time:	**Once** - Specifies the time of the day the scheduled task create the snapshot. **Every** - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.
Destination Path:	This will be the location where your duplication files will be saved. The default path will be the path of the share itself. You can change the path to the other shares except home and public. Duplication will follow the ACL settings of the destination share. If you set the destination of your home duplication to a public share then anybody can access that folders, so please be warned!
Snapshot Numbers:	Specifies the total number of snapshots that can be created. The maximum total number of duplication a share can have is 256.

NOTE: The destination space must be larger than the source. proNAS will check only the destination volume size, not the share usage. Be sure that the available space on the destination is reasonably big enough to accommodate any changes in the source. Home duplication is a special case. If the destination path of the home folder is set to the home itself, its duplication files will only be accessible via NFS or telnet service.

Create Duplication:	This button allows you to create duplication manually.
Delete All:	This button will remove all the duplication files of this share on the current destination path.
Enable / Disable Scheduled:	This button allows you to enable or disable a scheduled task.
Get List:	This button allows you to get the lists of duplications on the current destination path.

Creating Duplication Manually

To create duplication manually, first set the number of total duplication that will be created, set the destination path and then click the "CreateDuplication" button. The source share must have at least a single file in order for the duplication to work properly.

Removing or Clearing All Duplication Files

To delete all the duplication files of this share on the current destination path, press the "Delete All" button. Duplication files on the previous destination path will not be removed. Duplication files of other shares on the same destination path will not also be removed.

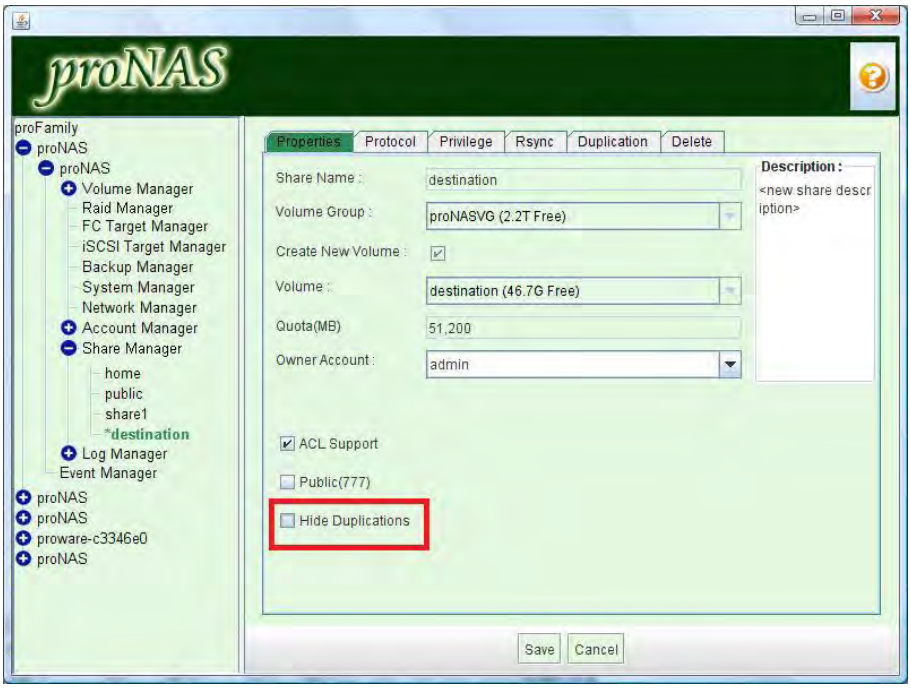
Getting the Duplication List

To get the lists of all duplication files of this share on the current destination path, please click the "Get List" button. The table will then update the lists of duplication folders. The table includes the date and time it was created and the destination path where it was saved. Duplication files of this share on the previous destination will no longer be included in the list. However proNAS will automatically update the duplication list for you every minute.

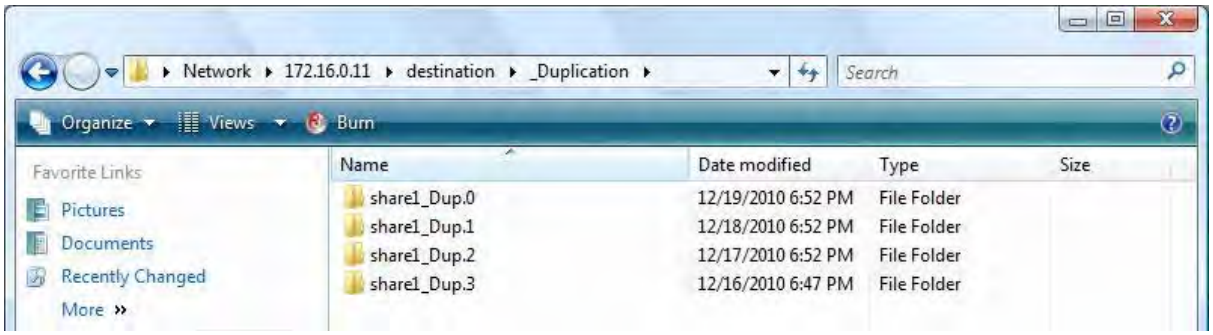
How Duplication Works

After you have created Duplication, your destination path will contain a folder "._Duplication". (It is hidden by default, to unhide it, uncheck the "hide duplication" option in the Properties tab of the destination folder). Inside the "._Duplication" folder are the directories that are created for the various intervals when Duplication was created.

Duplication created in “share1” share folder and destination path is “destination”



The share folder “destination” with “Hide Duplications” unchecked



Inside each of these folders is the full backup of that point in time of the source share. The format of the duplication folder name will be the share name of the source share appended by an underscore then the character "Dup" followed by the number of the interval. "ShareName_Dup.0" will always contain the most recent snapshot and the duplication with the highest interval number will contain the oldest snapshot. When a new duplication is run, it will rotate all the duplication directories. The files on oldest duplication will not be saved and will be replaced with the content of its succeeding duplication, so please take note of this. The number of duplication will depend on the number of snapshots that you have defined. You need to increase the total number of snapshots if you want to save the backups for a longer time. For example, if you set the snapshot numbers to 60 and you set a schedule to take duplication every day, the very last backup would be around two months old before it will be discharged if a new duplication is made.

NOTE: To view the date modified of duplication folders that corresponds to the date the duplication is taken, use File Manager and view in detailed mode.

5.6.7 Default Share

Basically, there are there are only two default shares when proNASVG is initially created. If the proBackup Service is started, two other default shares are created. The default shares in proNAS are:

- home - holds the individual shares of all users. It cannot be deleted.
- public - a share intended for all users. Any type of user (including guests or anonymous) can logon to this share and is given read-write permissions.
- proBackupDevice - holds the major backup device for proBackup application. It becomes visible after proBackup service is enabled.
- proBackupExtendedDevice - holds the extended device for other proBackup servers to utilize. It becomes visible after proBackup service is enabled.

5.6.8 Recycle Bin

The Recycle Bin function allows temporary storage of deleted files accessed via CIFS.

To enable Recycle Bin:

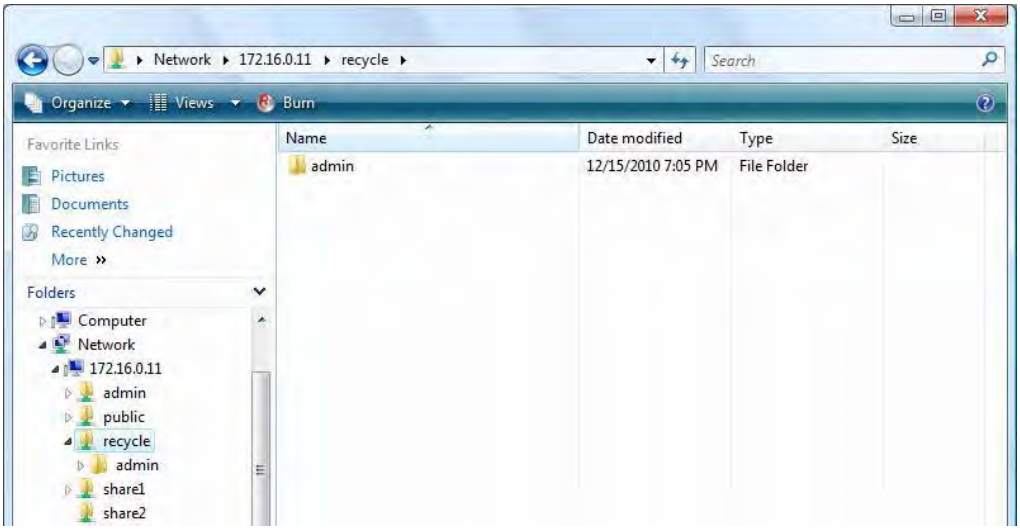
1. Click Share Manager and click “Options” tab. Click “Edit” and tick “Enable Recycle Bin”.

2. Select/modify volume to save or days to keep as necessary. Click “OK” when done.

NOTE: A separate Volume can be created for recycle bin use and then select it in “Select Volume to save” option. Or an existing Volume with share folder can also be selected in “Select Volume to save”, in which case the total capacity of the Volume will be shared by the “RECYCLE” folder and the other existing share folder.

3. To enable Recycle Bin option on a Share, select the Share name and click Protocol tab. Click “Edit”. Under CIFS, tick “Enable Recycle Bin”. Click “Save”.

4. When files are deleted from the share with enabled Recycle Bin, the files will be placed in the recycle share folder in the NAS.



Recycle folder containing the folder of “admin” account and the deleted files by admin

5.6.9 Audit

The Audit function allows saving audit log for share folders accessed via CIFS.

To enable Audit:

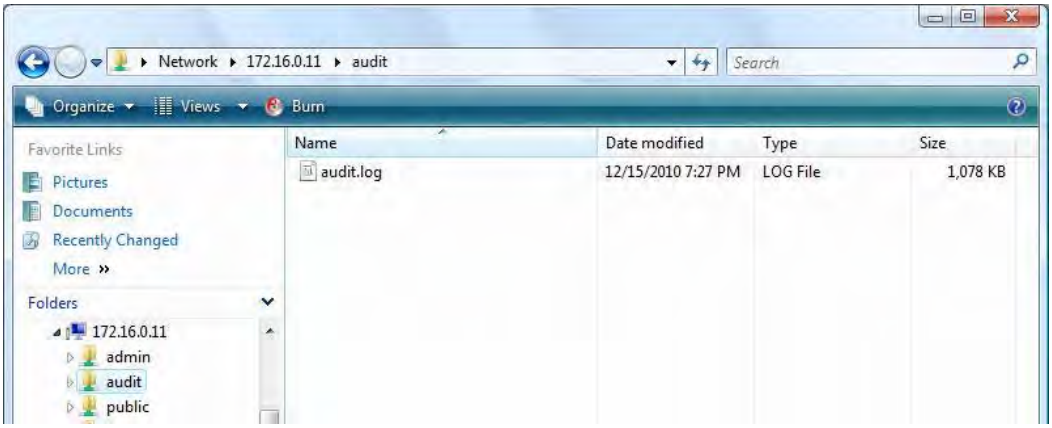
1. Click Share Manager and click “Options” tab. Click “Edit” and tick “Enable Audit”.

2. Select/modify volume to save or days to keep as necessary. Click “OK” when done.

NOTE: A separate Volume can be created for Audit use and then select it in “Select Volume to save” option. Or an existing Volume with share folder can also be selected in “Select Volume to save”, in which case the total capacity of the Volume will be shared by the “AUDIT” folder and the other existing share folder.

3. To enable Audit option on a Share, select the Share name and click Protocol tab. Click “Edit”. Under CIFS, tick “Enable Audit”. Click “Save”.

4. The audit.log file will be created in the audit share folder in the NAS.



A sample Audit log file

```
Dec 15 19:27:45 localhost smbd_audit: admin|172.16.0.199|gerry-
nb|share2|pwrite|ok|Java/JRE_1.6.0_u17_Linux/jre-6u17-linux-i586-
rpm.bin
Dec 15 19:27:45 localhost smbd_audit: admin|172.16.0.199|gerry-
nb|share2|pwrite|ok|Java/JRE_1.6.0_u17_Linux/jre-6u17-linux-i586-
rpm.bin
Dec 15 19:27:46 localhost smbd_audit: admin|172.16.0.199|gerry-
nb|share2|pwrite|ok|Java/JRE_1.6.0_u17_Linux/jre-6u17-linux-i586.bin
Dec 15 19:27:46 localhost smbd_audit: admin|172.16.0.199|gerry-
nb|share2|pwrite|ok|Java/JRE_1.6.0_u17_Linux/jre-6u17-linux-i586.bin
Dec 15 19:27:46 localhost smbd_audit: admin|172.16.0.199|gerry-
nb|share2|pwrite|ok|Java/JRE_1.6.0_u17_Linux/jre-6u17-linux-i586.bin
Dec 15 19:27:46 localhost smbd_audit: admin|172.16.0.199|gerry-
```

Sample contents of Audit log file

5.7 System Manager

System Manager is composed of different tabs which is responsible for the configuration of proNAS system settings and services, such as: Firmware Upgrade, Account and Share reports, Date and Time Zone, Serial Ports and UPS settings, Reboot functions, and Services configurations.

NOTE: Some information shown in the above screenshot may be different from your actual NAS system.

5.7.1 Information tab

The Information tab shows the account, storage and system information.

Account Information

- **Account Numbers** - Indicates the total numbers of all local and external accounts.
- **Share Numbers** - Indicates the total number of all shares.

Storage Information

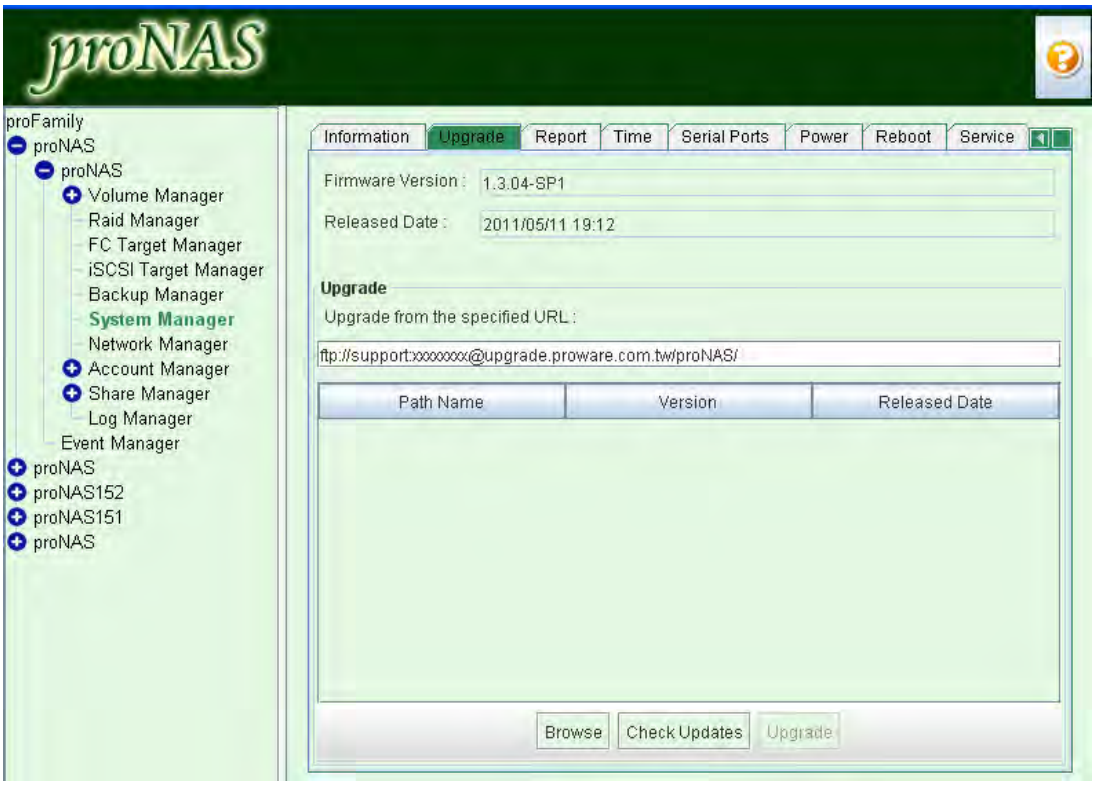
- **Disk Numbers (Free/Total)** - The number of disks in the subsystem, "Free" means the disks those are not joined in volume group.
- **Vol Group Numbers** - The total number of volume groups.
- **Volume Numbers** - The total number of logical volumes. Snapshots will also be counted as volumes.

System Information

- **Model -** shows the proNAS system model type.
- **Build Version** – shows the current proNAS firmware version.
- **CPU** - shows the CPU Type and the number of CPUs.
- **MHz** - shows the CPU speed.
- **Memory** – shows the RAM size.
- **NIC** – shows the NIC status, MAC address and IP address.
- **CPU Temperature -** shows the current CPU temperature
- **FAN information –** shows the system FAN speed

5.7.2 Upgrade tab

The Upgrade tab is used to upgrade the proNAS system firmware version.

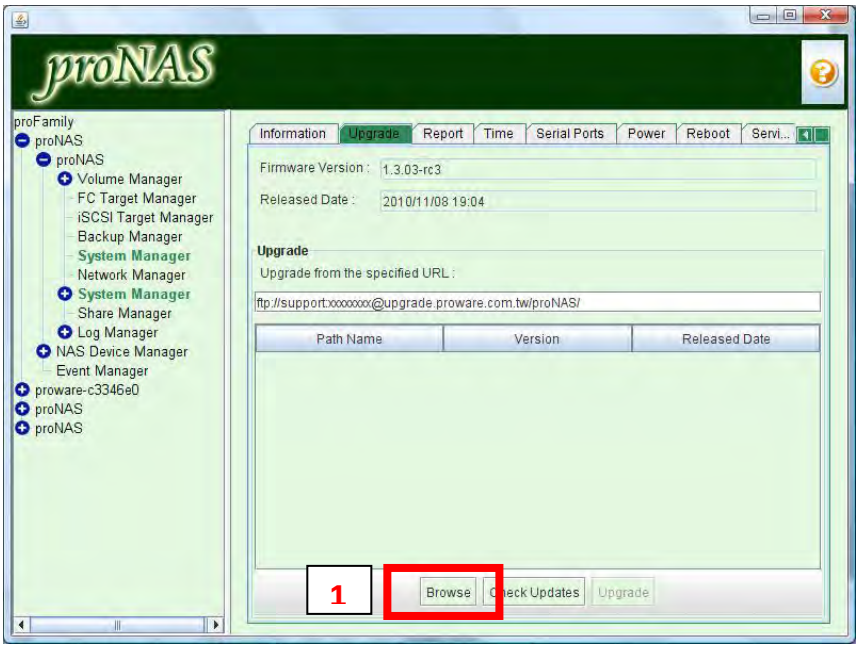


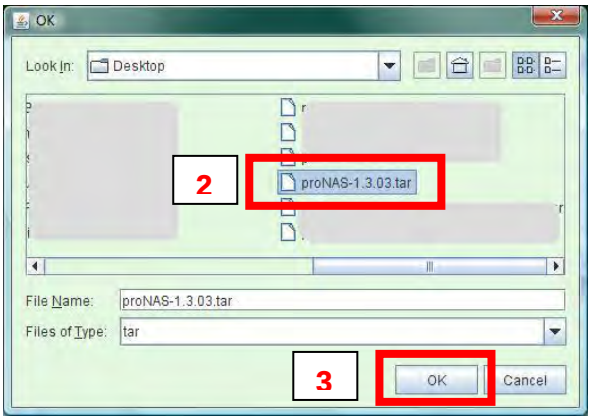
- **Firmware Version** - Displays the current firmware version.
- **Release Date** - The Release Date of this version.
- **Upgrade from the specified URL** - You can download the latest version from URL: ftp://support:xxxxxxxx@upgrade.proware.com.tw/proNAS/

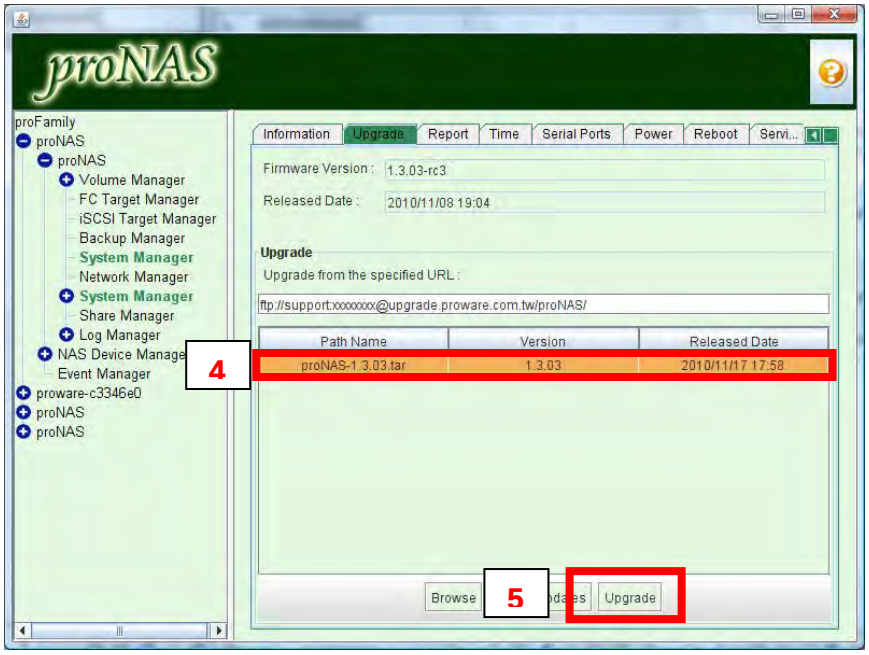
If you would like to see if there is latest version, please press "**Check Updates**" button. The system will search online (NAS should have internet connection) if there is any latest firmware to update. Then select (highlight) the proNAS tar file from the list, then click "**Upgrade**" button.

NOTE: During upgrade, the NAS system must not be in-use, which means the share folders, FC or iSCSI target volumes must not be accessed from client computers.

Aside from online firmware update from FTP site, you can also do a firmware update from local file system, but you need to download first the firmware tar file (for example: **proNAS-1.3.03.tar**) and save to the local directory of computer. Press the "**Browse**" button and locate the firmware tar file. Select the tar file when it appears in the list, then click "**Upgrade**" button. The NAS system will reboot to load the updates.

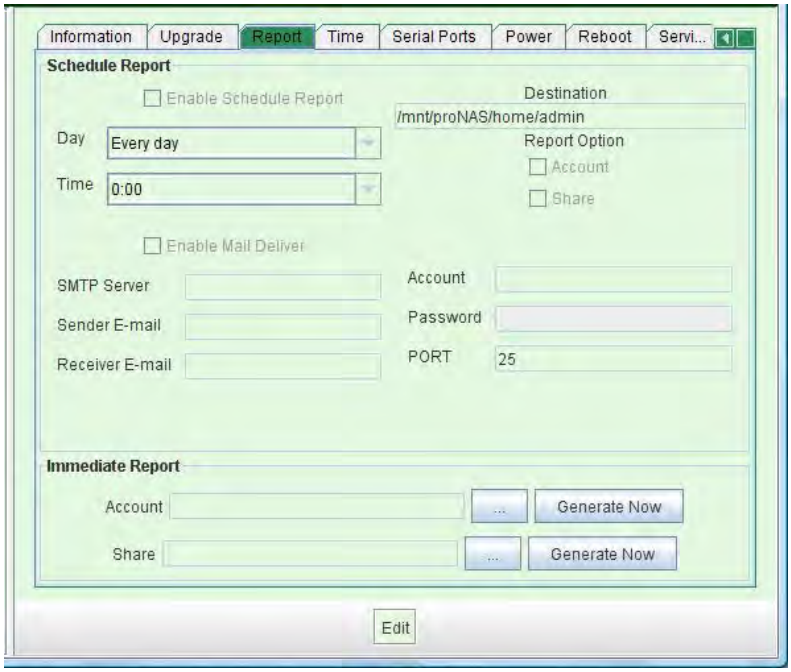

proNAS
proFamily
proNAS
proNAS
Volume Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
System Manager
Share Manager
Log Manager
NAS Device Manager
Event Manager
proware-c3346e0
proNAS
proNAS
Information
Upgrade
Report
Time
Serial Ports
Power
Reboot
Servi...
Firmware Version :
1.3.03-rc3
Released Date :
2010/11/08 19:04
Upgrade
Upgrade from the specified URL :
ftp://support:xxxxxxx@upgrade.proware.com.tw/proNAS/
Path Name
Version
Released Date
1
Browse
Check Updates
Upgrade


OK
Look In:
Desktop
2
proNAS-1.3.03.tar
File Name:
proNAS-1.3.03.tar
Files of Type:
tar
3
OK
Cancel


proNAS
proFamily
proNAS
proNAS
Volume Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
System Manager
Share Manager
Log Manager
NAS Device Manage
Event Manager
proware-c3346e0
proNAS
proNAS
4
Information
Upgrade
Report
Time
Serial Ports
Power
Reboot
Servi...
Firmware Version :
1.3.03-rc3
Released Date :
2010/11/08 19:04
Upgrade
Upgrade from the specified URL :
ftp://support:xxxxxxx@upgrade.proware.com.tw/proNAS/
Path Name
Version
Released Date
proNAS-1.3.03.tar
1.3.03
2010/11/17 17:58
Browse
5
Upgrade

5.7.3 Report tab

proNAS provides report function which enables you to collect the usage information of all accounts and shares. The output file will be saved in a ".csv" file. Report function can generate report either by schedule or immediately.



Schedule Report

If you would like to enable schedule report, press the "Edit" button, check "Enable Schedule Report", check the report option for "Account" or "Share" or both, and set the Day and Time when to generate the report. The system will generate the report and save in the path /mnt/proNAS/home/admin (The path can be modified).

If you would like to receive the report by e-mail, please check "Enable Mail Deliver" and input the information for SMTP server, sender e-mail and receiver e-mail address. If you prefer to enable email authentication, enter the account and password. You can also change the default port if needed.

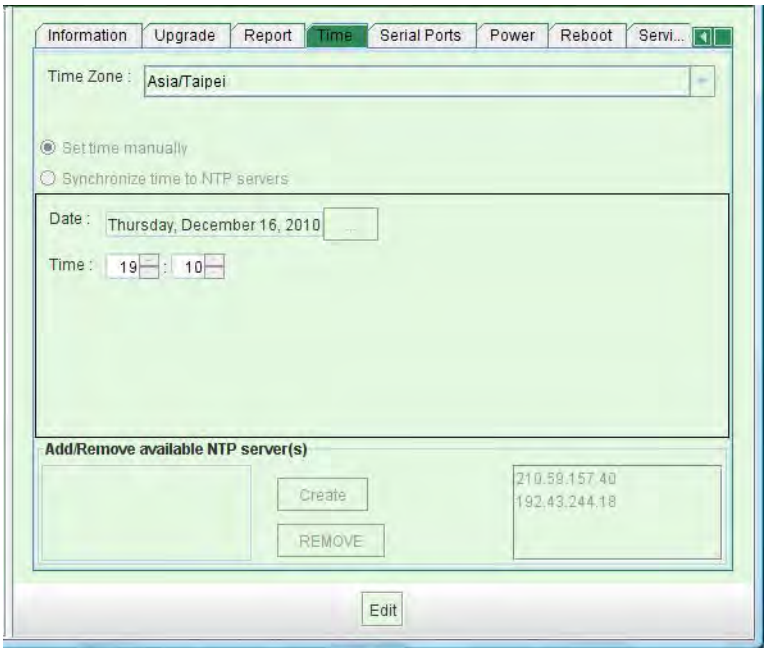
Immediate Report

If you would like to collect the report immediately, press "..." and choose the path for the output file and press "Generate Now" button.

5.7.4 Time tab

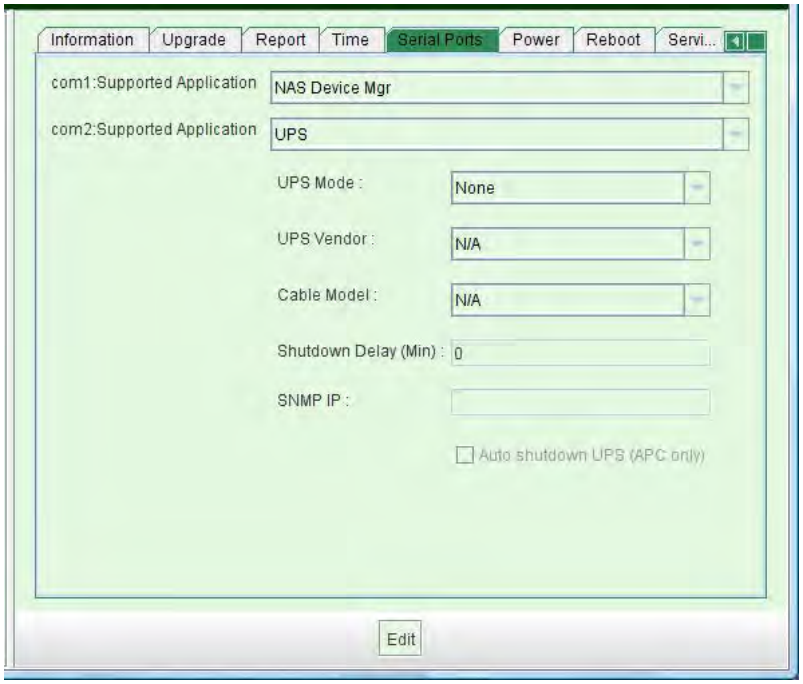
You can configure the system time, date and time zone in this tab. Click the "Edit" button and choose the appropriate time zone. After setting the time zone, select "Set time manually", if not selected, and then set the Date and Time. To set the date, press "...", then the system will display a calendar to choose the date. To set the time, change the hours and minutes.

If you would like to synchronize time with NTP server, select "Synchronize time to NTP servers". The system will display two NTP servers by default. If you would like to add NTP server, enter the NTP server IP address in the “Add/Remove available NTP server(s)” box and press "Create" button. The NTP server will appear in the list of NTP servers on the right column. To remove an NTP server from the list, select the NTP server IP address then press "REMOVE”. When the settings are completed, press "Save" button.



5.7.5 Serial Ports tab

Com1 and Com2 Serial ports can be configured in this tab for specific application. Press "Edit".



Com1

Supported Applications are: NAS Device Mgr or proNAS HA

Com2

Supported Applications are: UPS or proNAS HA

When Com2 is set to UPS, the following options can be setup:

UPS Mode: Dumb UPS or **UPS** (smart)

If Dumb UPS is selected, you don't have to configure the setting about vendor and cable.

If UPS (smart mode) is selected, you can choose from the three supported UPS vendors.

UPS Vendor: (a) **APC**, (b) **Beam-Tech**, or (c) **HyperPro**.

APC has many APC smart UPS models supported. Beam-Tech UPS model supported is SSpro 650. HyperPro UPS model supported is 1410HP.

If you select APC, you can select the Cable Model from the 5 options.

NOTE: Customers must use only the supported UPS vendor models: APC, Beam-Tech, and HyperPro. If other UPS models are used, there is no guarantee that the NAS will be able to communicate to the UPS. The basic UPS function (to provide uninterrupted power supply to the NAS) will probably work but the Shutdown Delay might not work using the UPS cable from the "unsupported" UPS vendor model.

Cable Model: (APC) **simple**, **smart**, **ether**, **usb**, or **snmp**
Please refer to the APC UPS specification for the UPS cable type used in the particular APC UPS model.
(Beam-Tech) **M2501** (default and cannot be changed)
(HyperPro) N/A (no need to specify)

Shut Down delay (Min): Use this option to set the delay time in minutes. After a power failure, UPS will shutdown the NAS when the Shutdown Delay time has expired.

NOTE: For most cases, it is recommended to use a value of 1 instead of 0 (zero) in Shutdown Delay.
When set to 0, the timer is disabled and the UPS will shutdown the NAS depending on the battery level and/or remaining runtime, or when the UPS battery is exhausted.
However, some types of UPS cables, which do not support low battery detection, might not work when Shutdown Delay is set to 0.

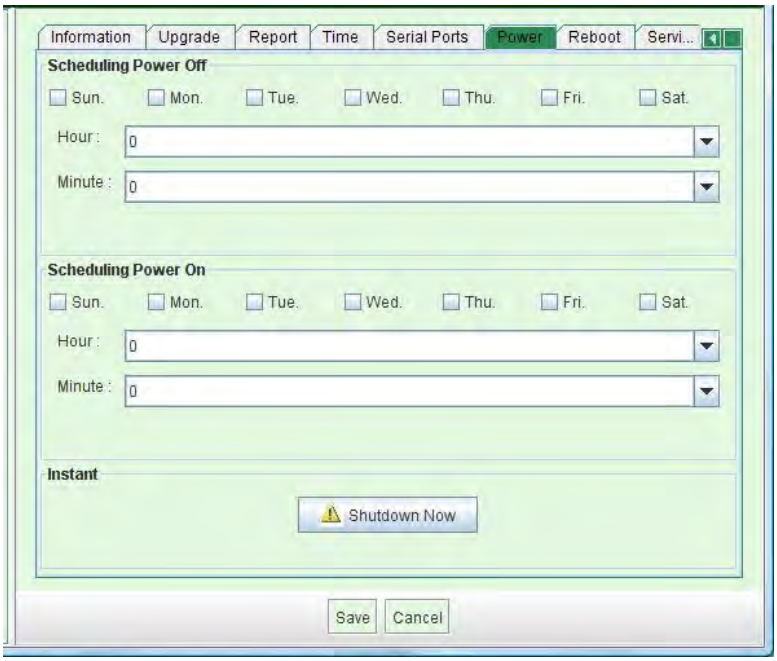
SNMP IP: the IP address of APC UPS. This is enabled when cable model is set to “snmp”.

Auto Shutdown UPS (APC only): this will automatically shutdown the NAS system after power failure; applies only to APC UPS

After completing the settings, press "Save" button.

5.7.6 Power tab

The Power tab is used to configure schedule system power off and power on. You can also shutdown the system immediately using “Shutdown Now” button.



Scheduling Power Off

Select the day or days, and set the Hour and Minute when the system will shutdown.

Scheduling Power On

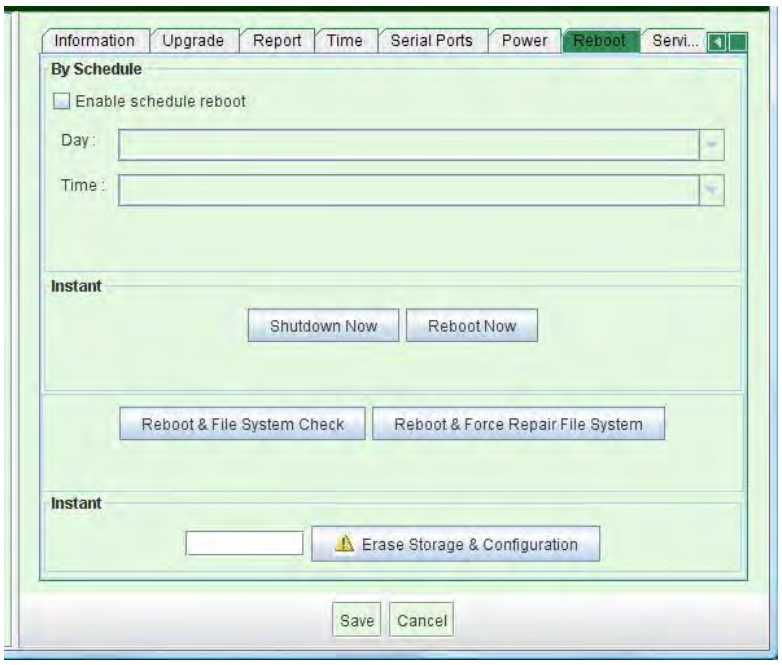
Select the day or days, and set the Hour and Minute when the system will power on.

Instant

To shutdown the NAS immediately, click “Shutdown Now” button.

5.7.7 Reboot tab

The administrator can reboot proNAS by schedule or immediately.



If you would like to reboot by schedule, press "**Edit**" button, and check "**Enable schedule reboot**". Choose the date and time when to reboot. This function can help to clean the unnecessary system process or connection periodically.

If you would like to shut down or reboot immediately, press "**Shutdown Now**" or "**Reboot Now**":

If you check there is file error or I/O error from system log, or VG cannot mount, or system shutdown abnormally, it is recommended to use the function "**Reboot & File System Check**".

If after using the option "Reboot & File System Check", there is still file system problem using, you can use the other option "**Reboot & Force Repair File System**" to force file system repair during reboot.

If you would like to erase existing storage and proNAS configuration and reset to factory default, you can use the "**Erase Storage & Configuration**" button.

WARNING! All data and configuration will be deleted if you use this function. Please make sure you already have a backup of your data and configuration, or that you do not need the current data and configuration.

5.7.8 Service tab

The various proNAS services can be set in this tab.

If you would like to enable service while booting, please check "Enable on Boot" option. You can also press "Start All Services" button to run all services, or press "Stop All Services" button to stop all services. If you would like to enable or disable certain service, please select the service item and press "Start" button or "Stop" button.

proNAS system services are as follows:

Samba services:	Provides CIFS file sharing, MS Windows users need this to access proNAS.
NFS services:	Provides NFS file sharing, UNIX users need this to access proNAS.
AFP services:	Provides AFP / AppleTalk service. Users need to enable this service to connect to NAS share folder via AFP/AppleTalk.
RSYNC server:	Provides Rsync process or system to which the Rsync client connects. **NOTE: By default, charset is set to UTF8 in Rsync configuration.**
SSH server:	Provides remote management with more secure level via SSH.

File Manager server:	Us this to enable (start) or disable (stop) the File Manager web page service.
Apache Web server:	This provides web service for proNAS use. You need to enable this service always. The default port number used is 80.
WebDAV Services	Provides Web-based Distributed Authoring and Versioning (WebDAV) service. This enables users to access share folders via web (HTTP Protocol).
Telnet service:	Provides users access proNAS with Telnet **NOTE: By default, maximum number of Telnet connections is set to unlimited.**
FTP service:	Provides users access proNAS with FTP
Internet Gateway:	Provides Internet access.
UPS monitor:	If you would like to connect UPS, you have to enable this service.
SNMP service:	Provides SNMP service. proNAS can send trap messages if: - A logical volumes becomes almost full (ID 128) - A snapshot volume becomes almost full (ID 129) - A replication is disconnected (ID 130)
MRTG service:	Provides MRTG service to show system information, such as CPU loading, memory usage, disk I/O, and LAN port network statistics.
proBackup service:	Provides service for NAS users to backup their files to NAS. Refer to Chapter 11 for fore information.
proNAS HA service:	Provides NAS HA solution.

proNAS provides "**Quick Configuration**" for administrator to configure service parameters. Experienced administrator can also configure the advance settings in "Detail Configuration".

proNAS Quick Configuration options are as follows:

Samba Service

- Strict allocate setting – This option controls the handling of disk space allocation in the proNAS server. When strict allocate is set to “no” (default setting) the server does sparse disk block allocation when a file is extended.
- SMP PORT – use this to set the SMB ports used; default ports use are 445 and 139. You can set either 445 or 139 only, or both (default).

NFS Service

- Enable NFS V4 – use this option to enable/disable NFS version 4.
- Enable NFS V2 V3 – use this option to enable/disable NFS version version 2/3.

AFP Service

- Languages – use this to set the language option. Default is UTF8.

RSYNC server

- Use chroot – use this to enable/diable chroot support. If enabled (default is “yes”), chroot enables change of root directory.

SSH Service

- Allows root login via SSH service
- Enable SFTP

The default settings of 2 options are set to “no”. If necessary, change the setting from “no” to “yes” then click “Save”.

File Manager Server

- Languages – This option allows selecting the language to be used by File Manager. Options are: English and Traditional Chinese.

Apache Web Server

- IP Port – The port number used by Apache web server. Default port number is 80.

Telnet services

- Allows root login via Telnet - default setting is “no”. To allow root access via Telnet, change the setting from “no” to “yes” then click “Save”.

FTP services

- Allows root login via FTP - default setting is “no”. To allow root access via FTP, change the setting from “no” to “yes” then click “Save”.

SNMP Service

- Trap Receiver IP: Enter the IP address of the SNMP trap receiver.

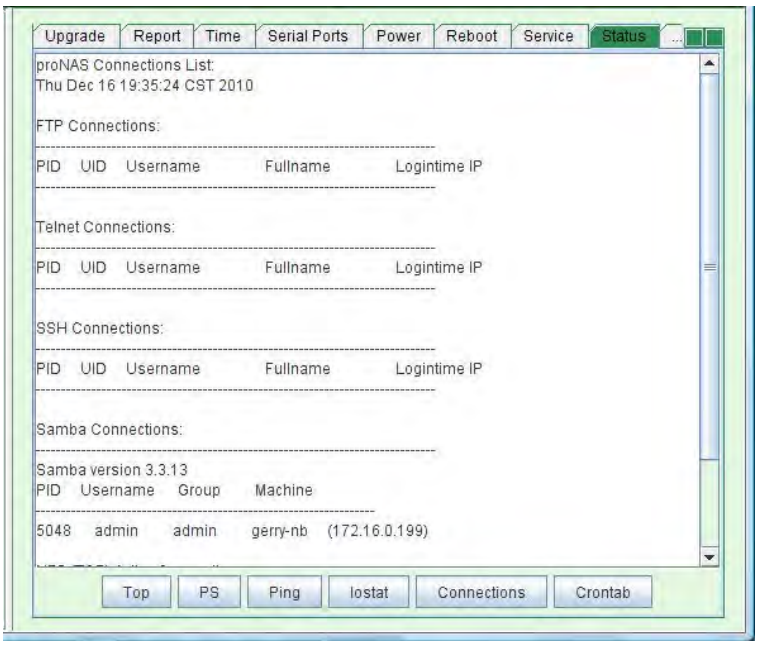
proBackup Service

- IP of Rx/Tx backup streams: Enter the proNAS network interface IP address for proBackup service stream
- Port of Rx/Tx backup streams: Enter the Port number for proBackup stream, default is 1089.

5.7.9 Status tab

You can use this tab to view system status, such as various Service Connections, Top, PS, and Iostat, to perform network test (Ping), or to view Crontab schedule.

By default, a summary of connections and resources used for local and remote computers is listed. The information includes the PID, User, User full name or comment, login time, and the IP address of the connected computer. You can click the "Connections" button to display current connection list.



Click the "**Top**" button to display system summary information and tasks list.

Click the "**PS**" button to display information about active processes.

Click the "**Ping**" button to perform network test. A dialog box will be displayed. Enter the IP address then click "Start". The ping result will be shown in the Status area.

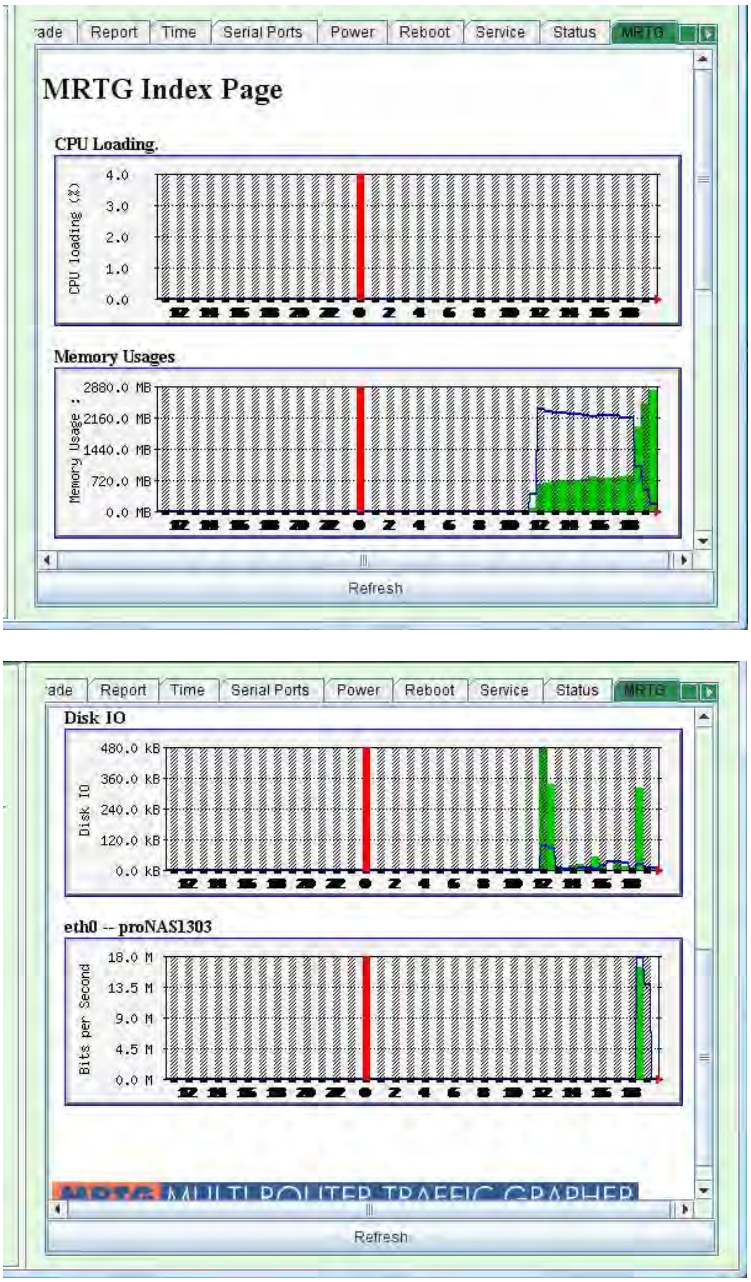
Click the "**Iostat**" button to display system input/output device loading, specifically storage and disk device statistics.

Click the "**Connections**" button to display current connection list.

Click the "**Crontab**" button to display a list of Crontab schedule.

5.7.10 MRTG tab

This tab shows information about MRTG graphs and includes CPU Loading, Memory Usage, Disk IO, and Network Traffic.

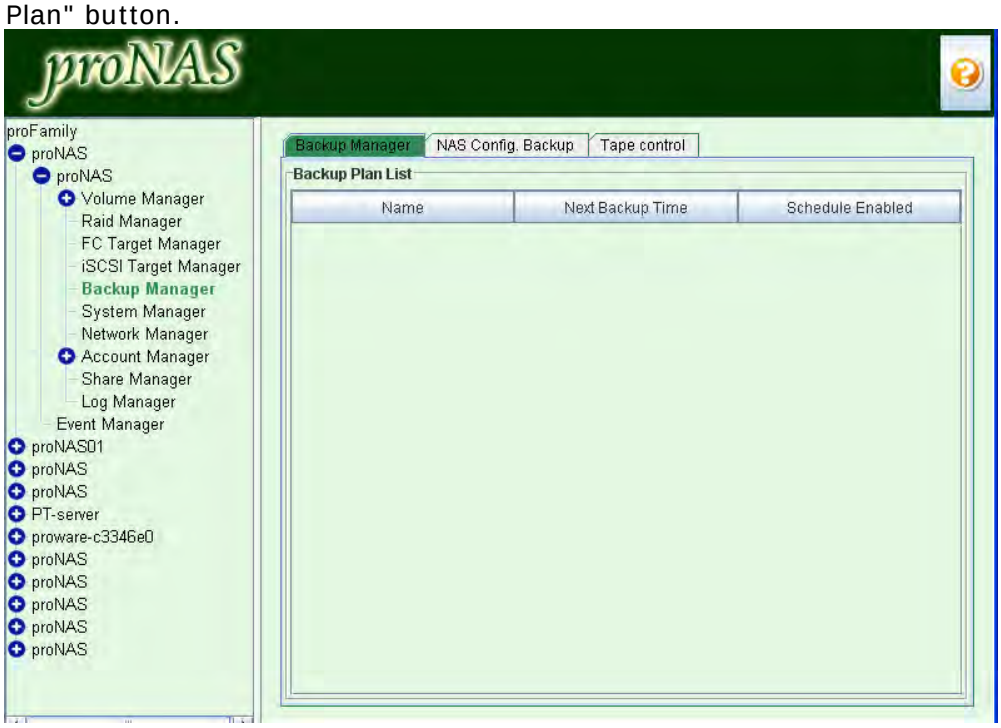


Sample MRTG graphs

5.8 Backup Manager

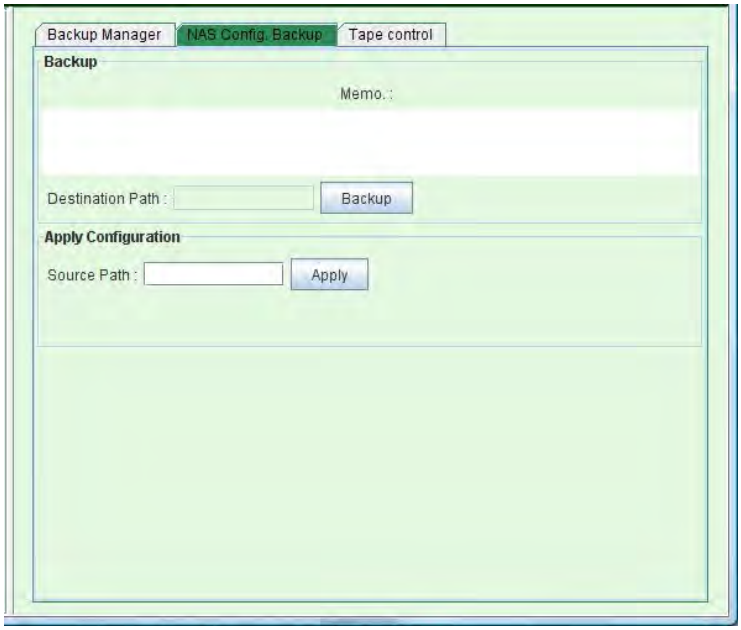
You can backup proNAS data and system configuration via Backup Manager.

In "Backup Manager" tab, you can check the existing backup plans in the "Backup Plan List" which includes backup plan name, next backup time and if the backup plan schedule is enabled. If you would like to create new backup plan, please press "Add Backup Plan" button.



5.8.1 proNAS Configuration Backup

proNAS provides System Configuration Backup which means administrator can backup system configuration information. Select "NAS Config Backup" tab.



Press "Backup" button. Choose the path you would like to save the file and enter the file name. System will backup the configuration information as an .xml file. If you would like to restore the configuration later, press "Apply" button.

NOTE: Not all proNAS configuration will be included in NAS Config backup. These includes Replication, Snapshot, Event Manager setting and HA configurations.

NOTE: Before you can restore a NAS backup configuration, you need first to reset the NAS to factory default settings. And make sure you have made a backup of all needed data.

5.8.2 Configure Backup Plan

Backup Plan Setting

In the "Backup Plan Setting" tab, you can create new a backup plan. Enter the "Backup Plan Name", and then press "..." to choose the backup destination, your destination could be remote share, tape or local device.

NOTE: If a disk is already selected as Local Device backup destination, the disk status in Volume Manager will change to "BACKUP". This disk will not be available in the Free Disks list at Destination option.

Use the following guidelines to ensure that you are using a valid backup plan name:

- Names cannot be longer than 256 characters.
- Names should be unique. It cannot be a duplicate with other Backup plan names.
- Names cannot contain blank spaces.
- Names cannot begin with a dash (-) and cannot consist of only a single dash.
- Names cannot contain the following characters: /\[]";:|<>+=,?*

If you choose remote share, please input the IP address in the "path" field. Choose Samba or NFS of the protocol and enter account and password.

Example:

For Samba:

Path = //192.168.100.164/Share	You cannot use the directory under the share. Example: //192.168.100.164/Share/dir1 <==Incorrect //192.168.100.164/Share <==Correct If you are not sure of the share name on the remote machine, you may query it by using the command "smbclient". -bash-3.00# smbclient -L 192.168.100.164
Login = account	Account that has full access permission on the remote share.

For NFS:

Path = 192.168.100.164:/PathToShareName	Example: 192.168.100.164:/mnt/proNAS/vol1/share1 If you are not sure of the correct path of the remote NFS server, you may use the command "showmount". -bash-3.00# showmount -e 192.168.100.164
Login	For NFS, it will assume the root account to be used. Please verify that root account can access the remote NFS share.

If Backup Manager fails to mount the remote share, you may need to verify it manually via console. That is to connect to the remote machine and mount the remote share. First we need to create a directory as our mount point.

```
-bash-3.00# mkdir /mnt/temp/
```

For Samba:

```
-bash-3.00# mount //ServerIP/ShareName /mnt/temp -o lfs,
                                    username=account,password=password
```

For NFS:

```
-bash-3.00# mount ServerIP:/PathToShareName /mnt/temp
```

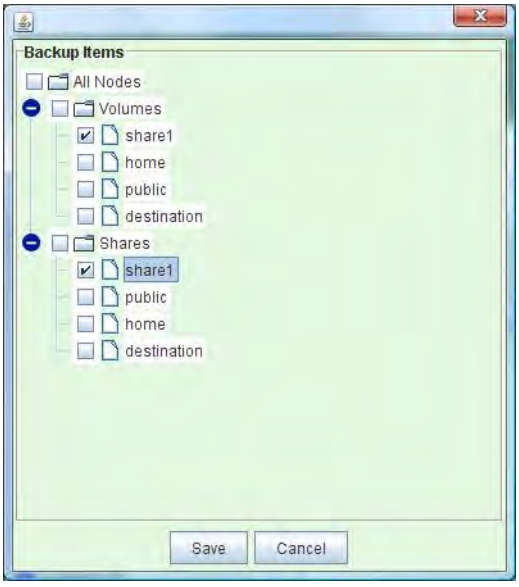
If you choose tape, you don't need additional setting.

If you choose local device, the system will display the available disks in the "Free Disk" field. When this backup configuration is saved, a “format local disk” confirmation window will be displayed.

If you choose the option "compressed", the data will be compressed to * .gz file.

Press "Save” button complete the setting and go back to "Backup Plan Setting" tab. In the field of "Description", system will display your backup destination (remote share / tape / local disk) in Type area.

Please press "Edit Backup Item List" button. System will display the window for you to choose the backup items ("Volumes" or "Share"). Choose your backup items and press "Save" button to go back to "Backup Plan Seting" tab. You can check the backup items in the "Backup Item(s)" list, if you would like to remove some items. Please check in the "Remove" filed and press "Remove Backup Item(s)".



Schedule Backup tab

After you complete the above setting, you can setup the schedule in the "Schedule Backup" tab, if the tab, you will see the option of "No Schedule", "Daily", "Weekly", and "Monthly".

- **Daily**: If you would like to do the backup every day, please check "Daily". Please press"...", system will display the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".

proNAS provides 3 kinds of backup methods:

- Incremental: An incremental backup stores all files that have changed since the last backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup is processed, which could result in a lengthy restore job.
- Differential: A differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup.
- Full: Full backup

- **Weekly**: If you would like to backup weekly, please check this option. Please press "...", system will displays the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".

- **Monthly**: Full backup is the starting point for all data backup. Choose this option to do full backup monthly.

Press "Save" after you completed the settings. Go back to "Backup Plan Setting" tab. You will see the backup plan in the "backup plan list".

If you would like to modify the backup plan, please choose the backup plan in the left tree-node, and press "Edit". If you would like to backup immediately, please press "Backup Now"; or press "Enable schedule backup". System will display schedule enable or disable in "Backup Status" field.
If you would like to restore data from the backup plan, please choose the backup plan in the left tree-node, and go to "Restore" tab, press "Restore" button.

5.8.3 Tape Control

The Tape Control tab allows you to control the tape function when attached to the NAS.

Options:

rewind tape to the begin. – This enables the tape to be rewound to the beginning of the tape.

forward tape to the end of data – This enables the tape to be forwarded to the end of data.

erase all data in tape – This enables the data on the tape to be erased.

eject tape – This enables the tape to be ejected from tape drive.

Status – This shows some information about current status of tape, such as tape is online.

When using the rewind/forward/erase/eject option, a confirmation message will be displayed. You can select “Yes” to continue, or “No” to cancel.

NOTE: Backup to tape has the following features:

1. **Backup across 2 tapes**

   When doing backup of large data and the first tape cartridge becomes full, the backup can continue by inserting another tape cartridge.

2. **Multiple backup**

   When doing backups, it can be done many times. That is, a backup plan can be executed many times and the backup data will be saved one after the other in the tape cartridge.

5.8.3.1 Backup and Restore Using Tape

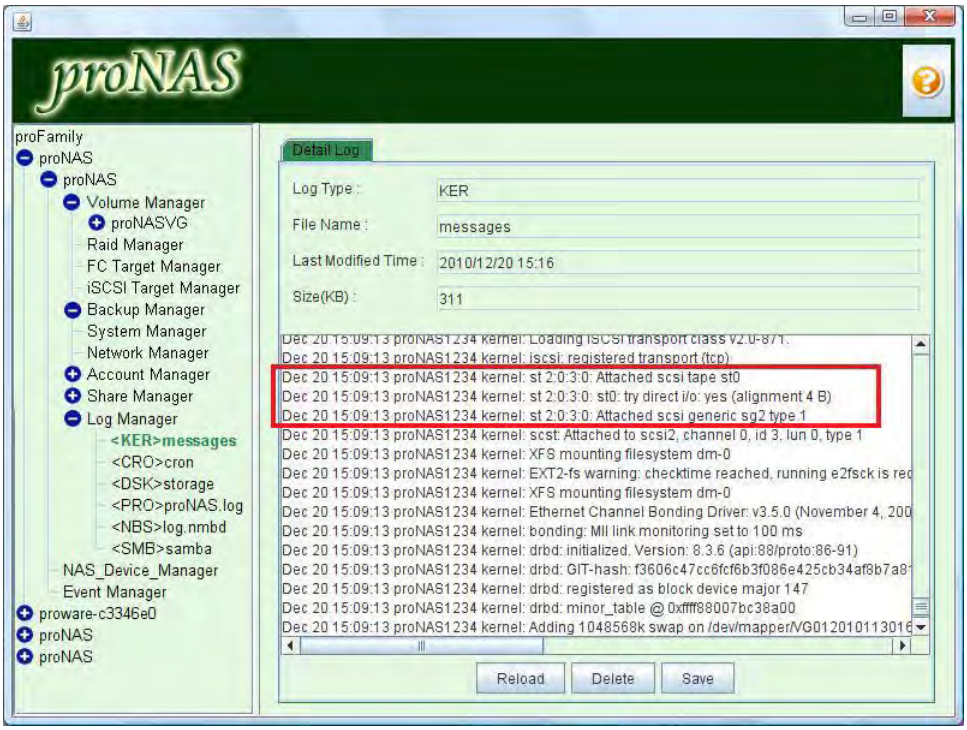
Here are sample procedures how to create backup to tape drive, or restore backup.

A. Preparing the NAS and Creating Backup Plan

1. Connect the Tape Backup device to the available Tape (SCSI) port on the NAS. Note that you need to shutdown the NAS before connecting the Tape Backup device.

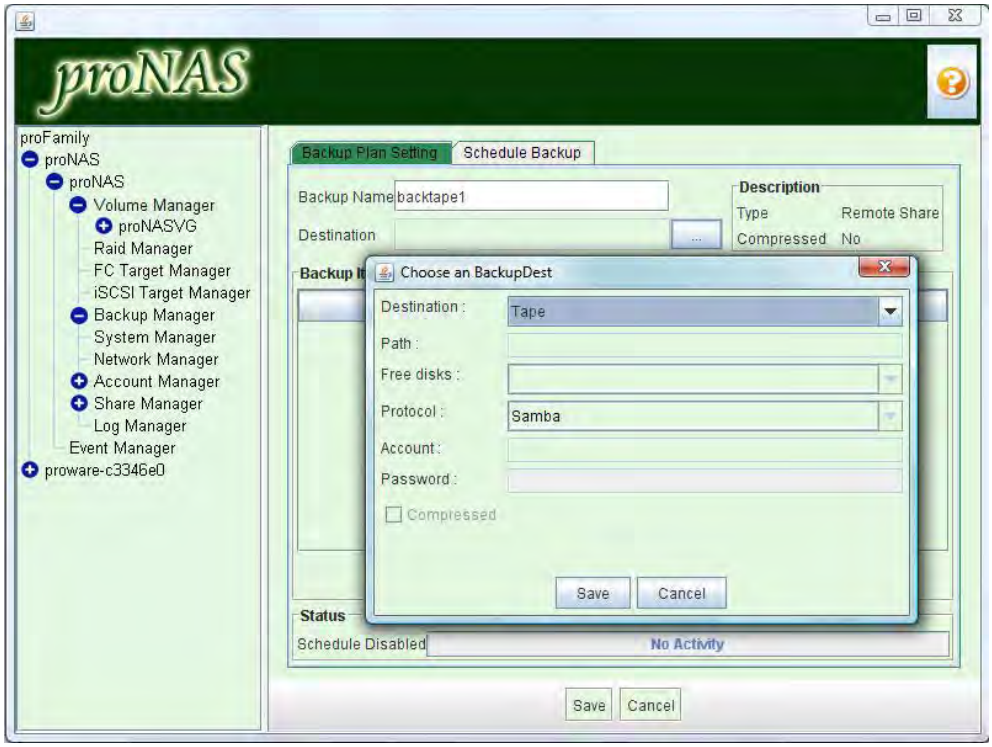
NOTE: Some NAS models do not have Tape port (external SCSI port). If the Tape Backup device connects via SCSI channel and the NAS model does not have an external SCSI port, a SCSI HBA needs to be installed in the NAS.
Some NAS models only have PCI-E expansion slot, while some have PCI-E and/or PCI-X. Please check with your storage vendor the expansion slot available in your specific NAS model before adding a SCSI HBA.

2. After boot-up of NAS, check in the Log Manager (<KER>messages) if the tape device has been detected. It should show device "st0".


proNAS
proFamily
proNAS
proNAS
Volume Manager
proNASVG
Raid Manager
FC Target Manager
iSCSI Target Manager
Backup Manager
System Manager
Network Manager
Account Manager
Share Manager
Log Manager
<KER>messages
<CRO>cron
<DSK>storage
<PRO>proNAS.log
<NBS>log.nmbd
<SMB>samba
NAS_Device_Manager
Event Manager
proware-c3346e0
proNAS
proNAS
Detail Log
Log Type : KER
File Name : messages
Last Modified Time : 2010/12/20 15:16
Size(KB) : 311
Dec 20 15:09:13 proNAS1234 kernel: iscsi: registered transport (tcp)
Dec 20 15:09:13 proNAS1234 kernel: st 2:0:3:0: Attached scsi tape st0
Dec 20 15:09:13 proNAS1234 kernel: st 2:0:3:0: st0: try direct i/o: yes (alignment 4 B)
Dec 20 15:09:13 proNAS1234 kernel: st 2:0:3:0: Attached scsi generic sg2 type 1
Dec 20 15:09:13 proNAS1234 kernel: scsi: Attached to scsi2, channel 0, id 3, lun 0, type 1
Dec 20 15:09:13 proNAS1234 kernel: XFS mounting filesystem dm-0
Dec 20 15:09:13 proNAS1234 kernel: XFS mounting filesystem dm-0
Dec 20 15:09:13 proNAS1234 kernel: bonding: MII link monitoring set to 100 ms
Dec 20 15:09:13 proNAS1234 kernel: drbd: initialized. Version: 8.3.6 (api:88/proto:86-91)
Dec 20 15:09:13 proNAS1234 kernel: drbd: registered as block device major 147
Dec 20 15:09:13 proNAS1234 kernel: drbd: minor_table @ 0xffff88007bc38a00
Reload
Delete
Save

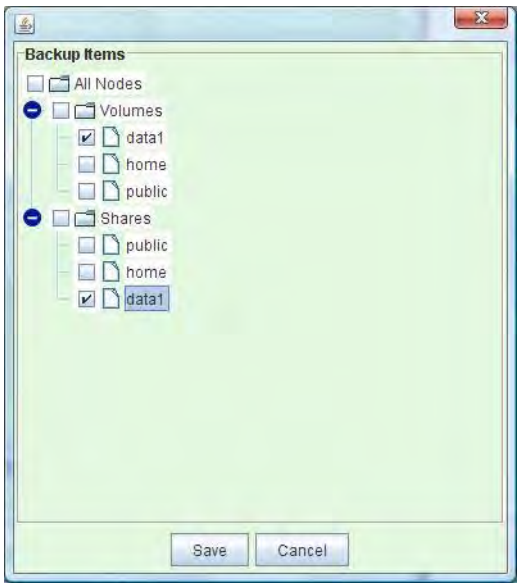
3. Select Backup Manager. Click “Add Backup Plan”.

4. Enter a Backup Name. In Destination, click “…” button. In the dialog box that appears, select “Tape” as backup destination. Click “Save”.



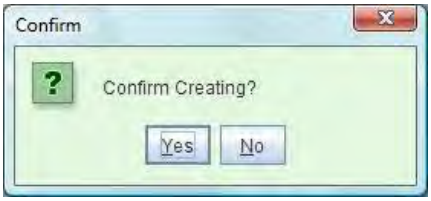
5. The destination (tape device) is set. Click “Edit Backup Item List”.

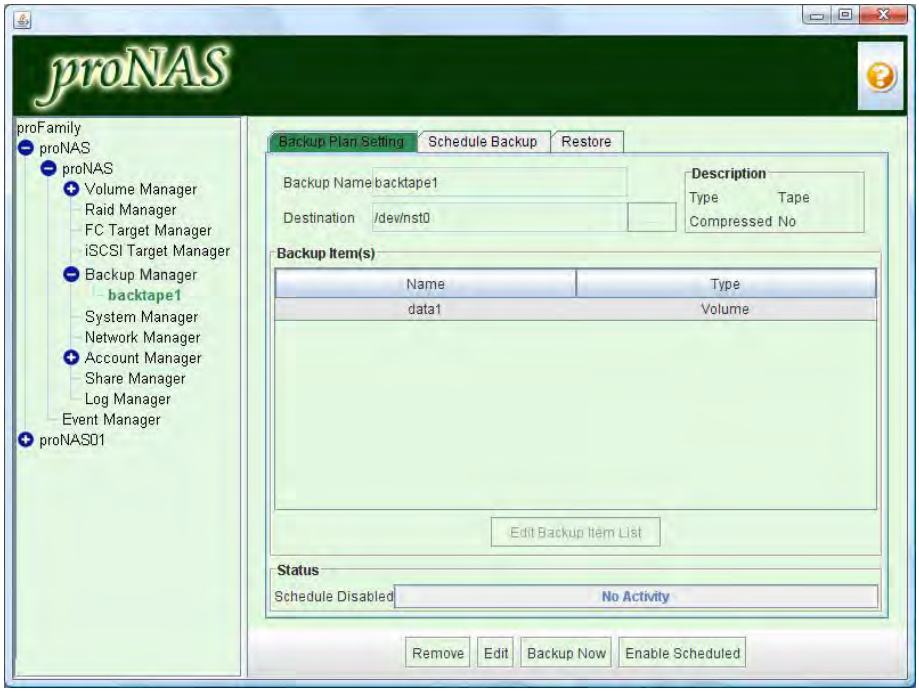
6. Select the data (Volumes/Shares) to be backed up. Click “Save”.



7. Click “Save” again.

8. In the Confirm Dialog Box, click “Yes”. The backup plan will be saved.





9. Insert the tape cartridge into the tape drive, if not yet inserted.

Take note of the following proNAS tape control functions as follows:

rewind tape to the begin. – This enables the tape to be rewound to the beginning of the tape.

forward tape to the end of data – This enables the tape to be forwarded to the end of data.

erase all data in tape – This enables the data on the tape to be erased.

eject tape – This enables the tape to be ejected from tape drive.

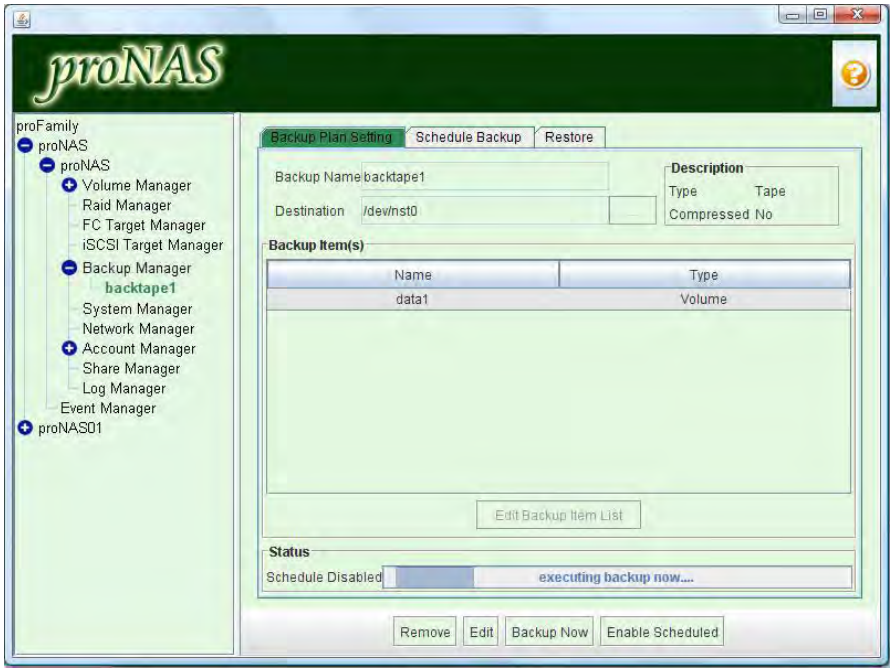
Status – This shows some information about current status of tape, such as tape is online.

B. Manual Backup and Restore

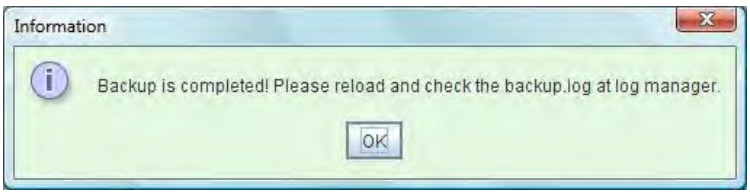
1. Select the backup plan under Backup Manager.

2. Click “Backup Now”. In the dialog box, click “Yes” to confirm.

3. The backup process will be started.

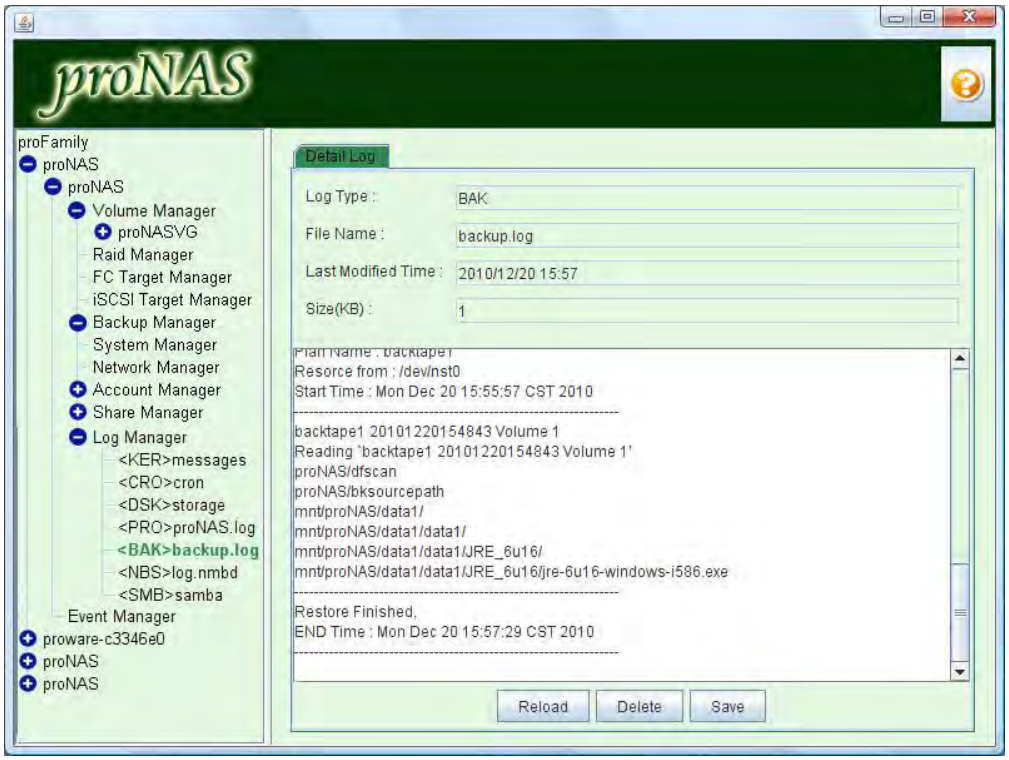


4. When backup is completed, a message will be displayed. Click “OK”.



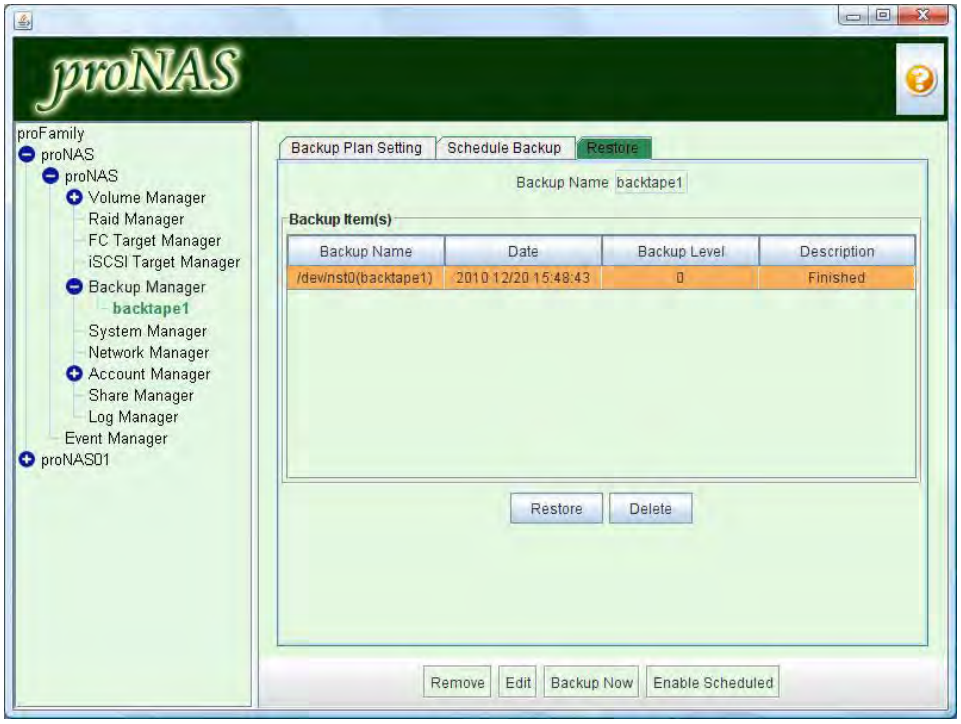
5. To check the backup made, while in the backup plan name, select the Restore tab.

To verify backup process from the log, select Log Manager then “<BAK>backup.log”. Note that you may need to click “Reload” to update the log information.



6. To restore data, try to delete old data from the share folder.

7. To restore data from tape backup, in Restore tab, select the backup name from backup Item(s) then click “Restore”.

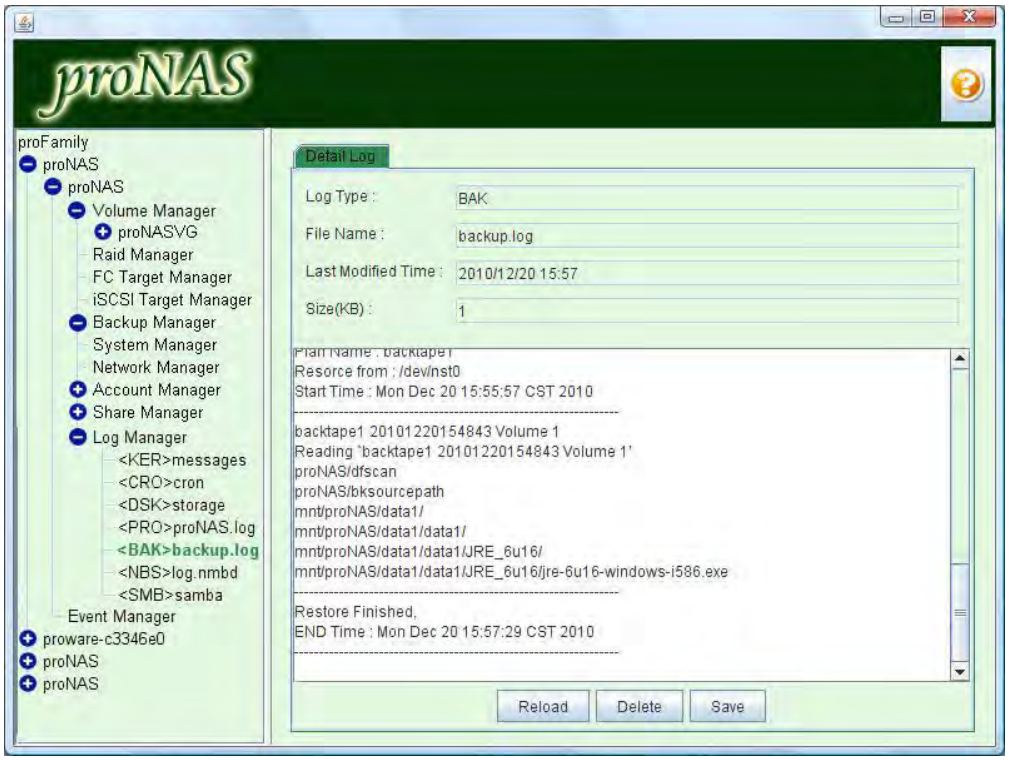


8. In the Confirm dialog box, click “Yes” to confirm.

9. The process of restoring data will be started.

10. When restore is completed, a message will be displayed.

11. To verify restore process from log, select Log Manager then “<BAK>backup.log”. Note that you may need to click “Reload” to update the log information.



12. Check the share folder if it contains the previous data that was restored.

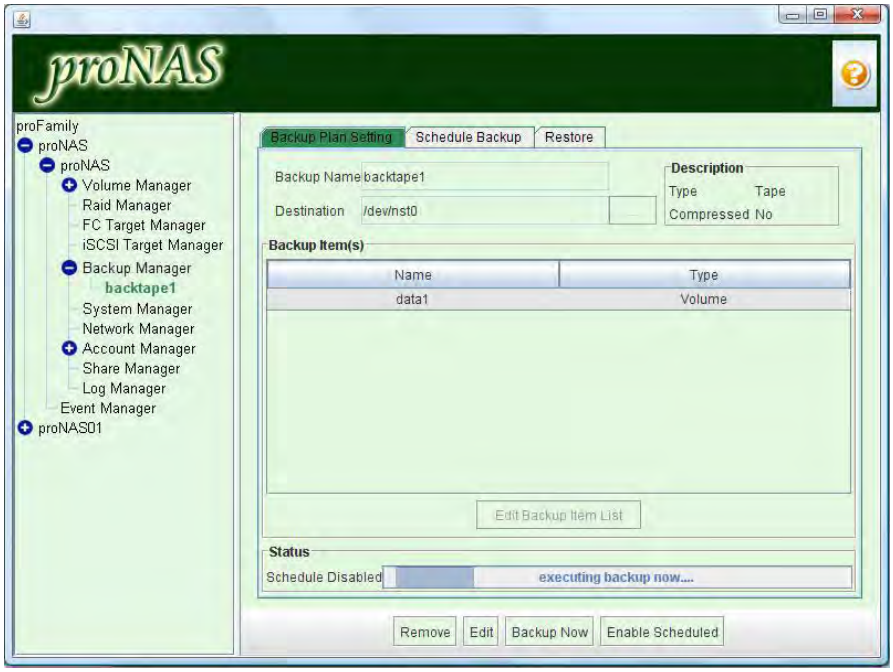
C. Creating Multiple Manual Backups

NOTE: Manual backups are always Full backup, which means their Backup Level is always 0 (zero).

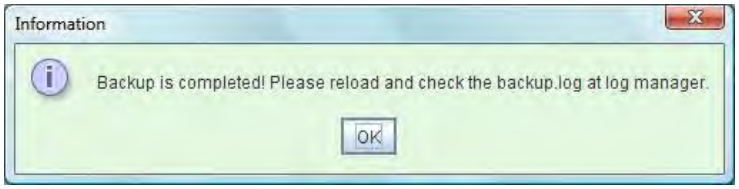
1. Update (copy and/or delete) some data to the share folder.

2. To create the first manual backup, select the backup plan then click “Backup Now”. Select “Yes” to confirm.

3. The backup will be executed.



4. A message will be displayed after backup is completed.



5. The first backup is created.

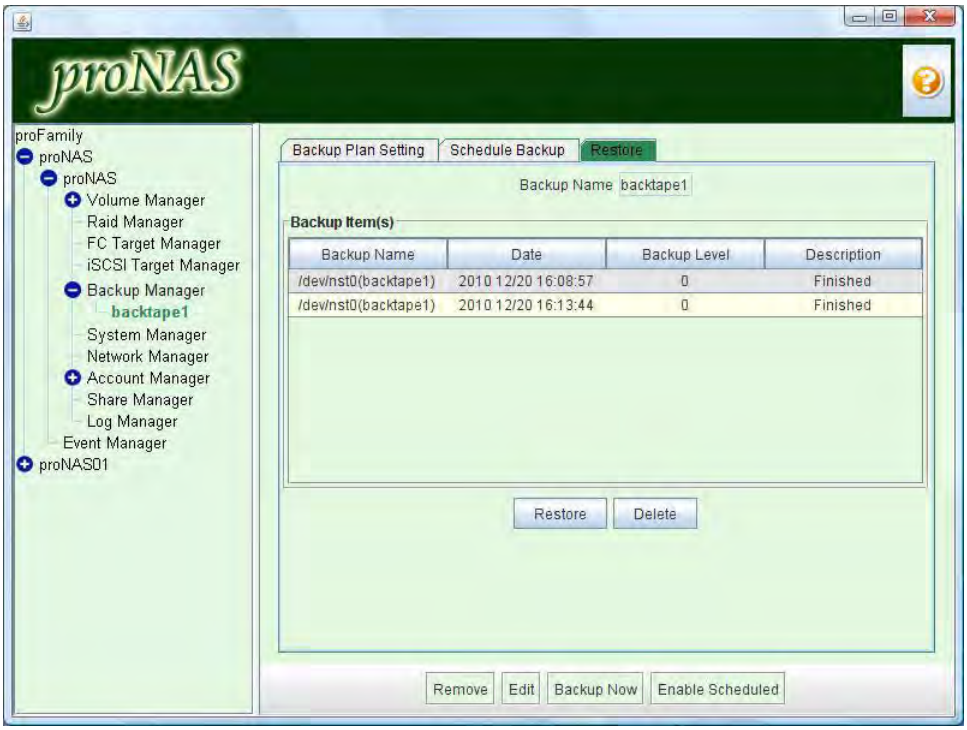
6. Update (copy and/or delete) some data to the share folder.

7. To create the second backup, click “Backup Now”. Select “Yes” to confirm.

8. The backup process will start.

9. When completed, a message will be displayed.

10. In Restore tab, check the backup items. A second backup item is displayed. Note that the Backup Levels are 0.

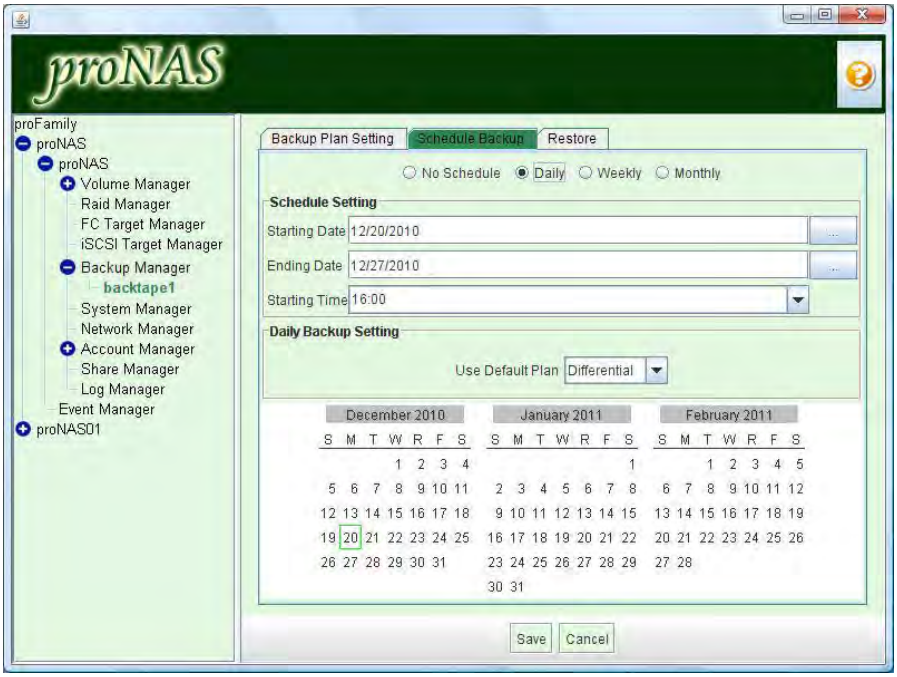


11. The backup items can be restored or deleted. If you need to create the third backup and so on, repeat steps 7 to 9.

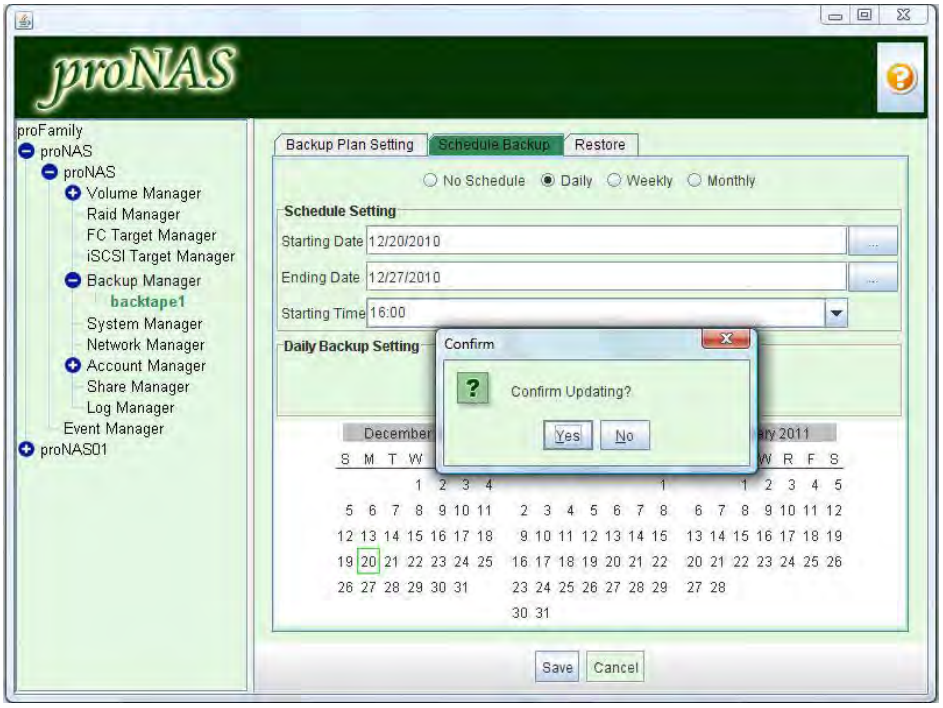
D. Backup by Schedule

1. Create a backup-to-tape backup plan (set destination to tape, and select backup items). Then click “Edit”.

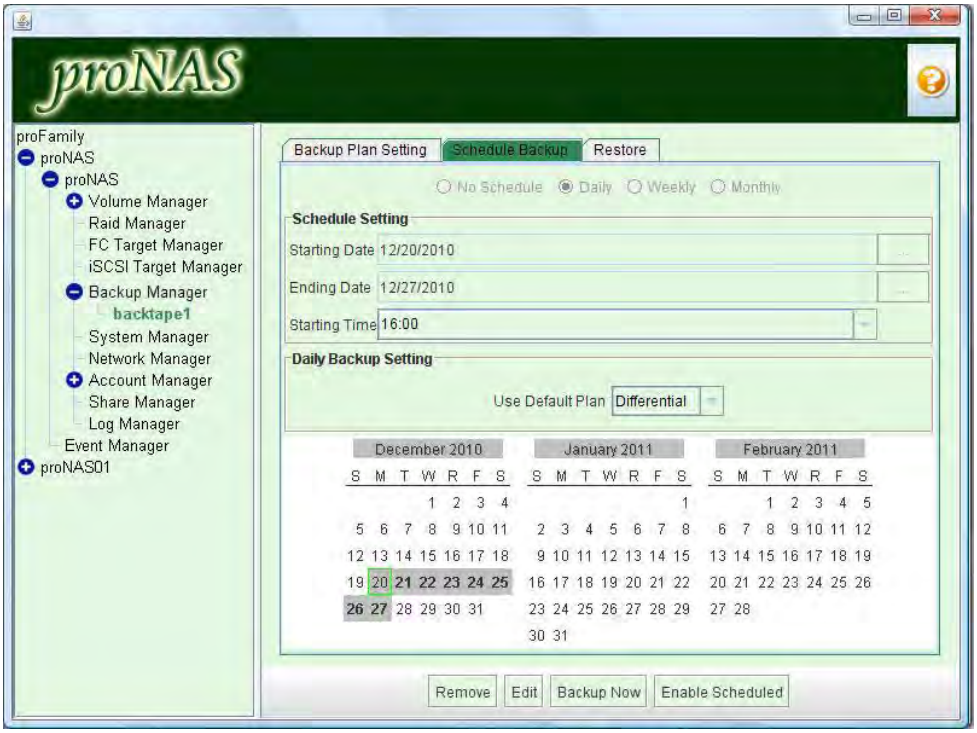
2. Select “Schedule Backup” tab. Select the backup frequency (Daily, Weekly, or Monthly). Set the starting date, ending date, and starting time. Specify the backup type in Use Default Plan option. For example, in Daily backup, you can select Differential, Incremental, or Full.



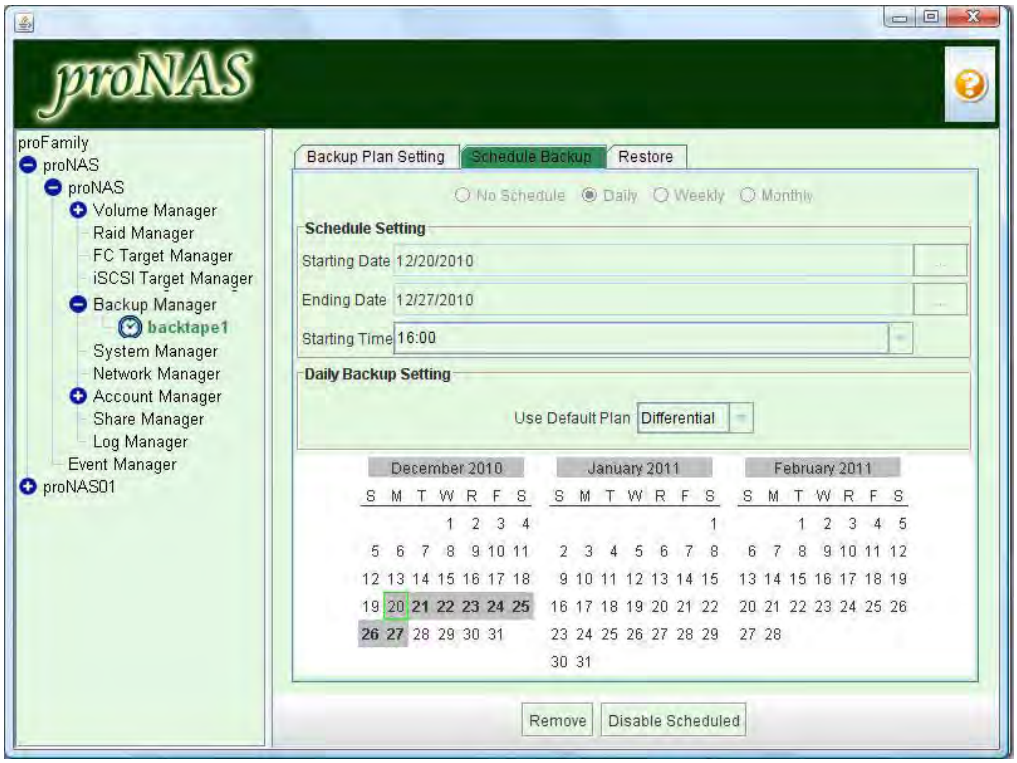
3. Click “Save” when done. Select “Yes” to confirm.



4. Scheduled backup has been configured.



5. To enable the scheduled backup, click “Enable Scheduled”. A clock icon will appear beside the name of backup plan.



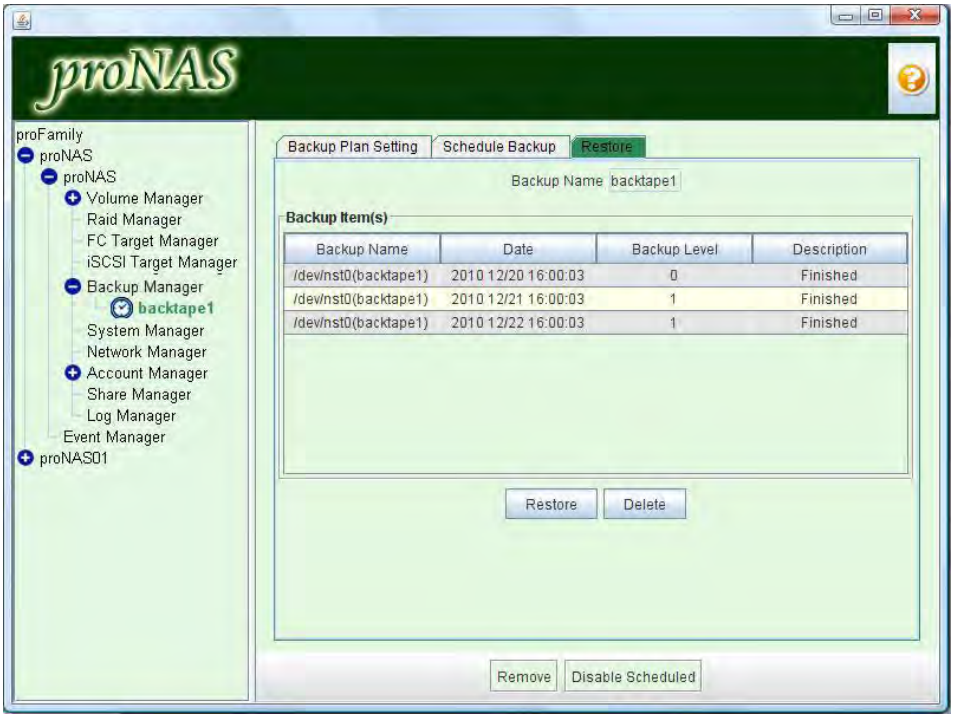
6. When the scheduled time comes, the backup will be executed.

7. Click “OK” to close the message. In Restore tab, check the backup name created.

8. In the succeeding schedule, next day for example (if backup is configured for daily backup) the backup will be created automatically.

9. Verify in Restore tab the backup items that have been created.

With Second Daily Backup



With Third Daily Backup

NOTE: The procedure for restoring backup from scheduled backups is the same as in manual restore. That is, select the backup item name from Backup Item(s) list and then click "Restore".

5.9 Log Manager

The Log Manager enables you to view the important logs generated by proNAS.

The Event List tab of the Log Manager lists the log type, file name, date and size (KB). To update the latest log information, press the **"Reload"** button.

Some of the types of log are:

KER - This log contains information about the Linux Kernel service. Its path is /var/log/messages. It can store information of 7 days. This log also contains information about NFS service.

CRO cron – This log contains information about cron daemon.

DSK - This log contains information about the changes to volume. Its path is /var/log/storage.log. It can store information of 7 days.

RDM – This contains the RAID Controller log.

CRO crontab – This contains Crontab information.

BAK - This log contains the status of Backup Manager.

PRO - This log contains information about proNAS service.

SMB - This log contains information about CIFS and Samba protocol. Its path is /var/log/samba.log

NBS – This log contains information about NetBIOS name server which provide NetBIOS over IP naming services to clients

RSY – This is the log for Rsync service.

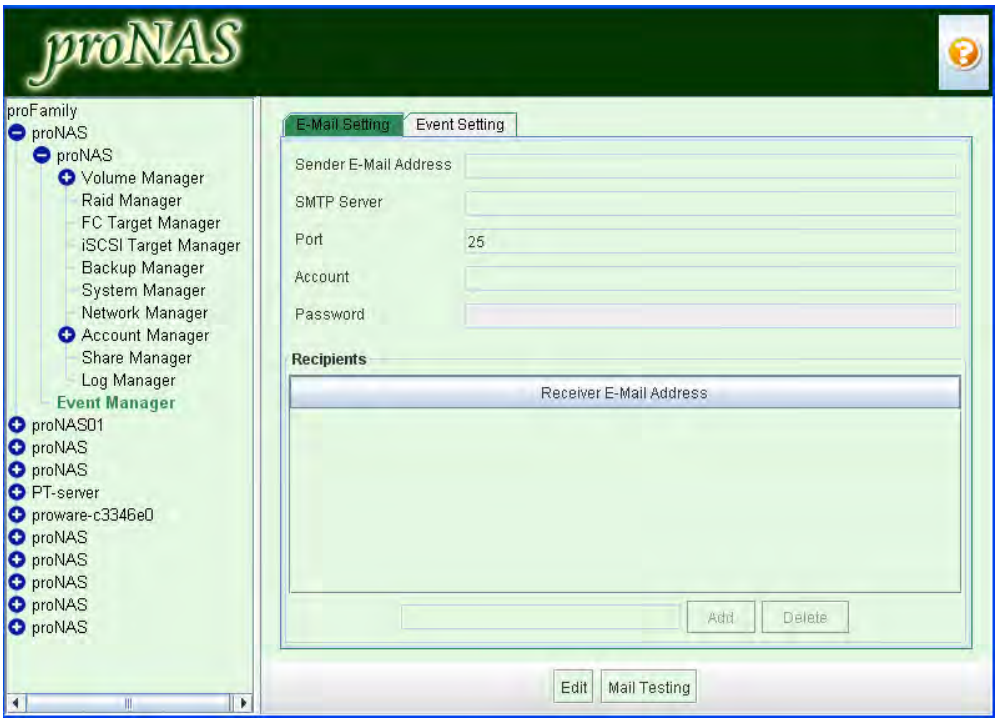
DUP - This log contains the information of the duplication function.

Save All Logs – This button allows you to download all log files and save to local folder or destination.

5.10 Event Manager

Event manager is a set of management wherein you can set to receive email notifications or trigger certain commands when a **proNAS**, **proNAS HA** or **Raid Manager** event occurs.

5.10.1 E-Mail Setting



Press "Edit" button to edit the following fields:

- **Sender E-mail Address** - Enter the sender's e-mail address.
- **SMTP Server** - Enter the IP address of the SMTP server.
- **Port** - Enter the port number. Default is 25.
- **Accounts** - Enter the SMTP server admin account.
- **Password** - Enter the SMTP server admin password.

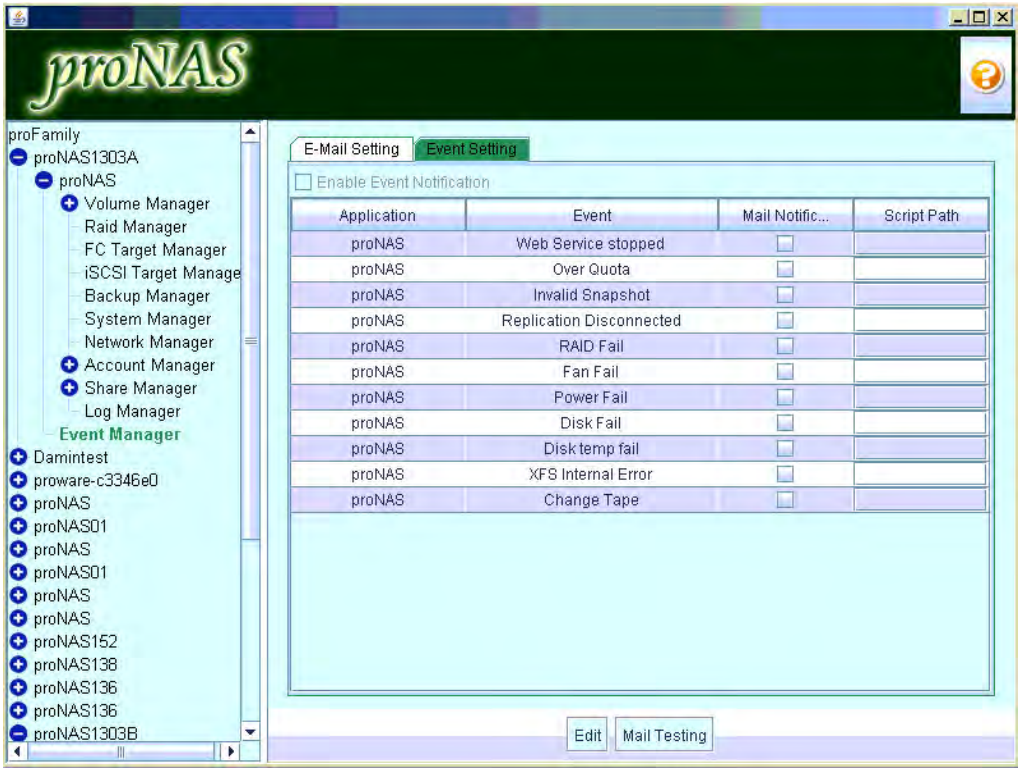
To enter a recipient's e-mail address, enter the e-mail address in the text box provided. Press "Add" button to insert the e-mail address in the Recipients list. You can have multiple recipients.

If you would like to delete a recipient, select the recipient's e-mail address and then press "Delete".

Click "Save" when done.

To verify if setting works, use the "Mail Testing" button to send a test e-mail.

5.10.2 Event Setting



Press "Edit" button and check the box "Enable Event Notification". Choose the following mail notification. The lists of event options will depend on which service is currently active. By default, all proNAS event will be displayed. Events for proNAS HA will be displayed only after you have started this service.

Event Options:

Press "Edit" button and check the box "Enable Event Notification". Choose the following mail notification. The lists of event options will depend on which service is currently active.

Some of the event options are:

Application	Event	Purpose
proNAS	Web service stopped	Notify if Apache web service is stopped.
proNAS	Over Quota	Notify if a logical volume exceeds the given quota (full or almost full). Please check the "Send email when not enough space" for the logical volume.
proNAS	Invalid Snapshot	Notify if a snapshot became invalid.
proNAS	Replication Disconnected	Notify if replication was disconnected.
proNAS	XFS Internal Error	Notify when NAS system encountered XFS Internal Error
proNAS	Change Tape	Notify to change backup tape
proNAS	RAID Fail	Notify if RAID fails
proNAS	Fan Fail	Notify if a fan fails
proNAS	Power Fail	Notify if a power supply fails
proNAS	Disk Fail	Notify if a disk drive fails
proNAS	Disk Temp Fail	Notify if disk drive over-temperature happens

Other event options are:

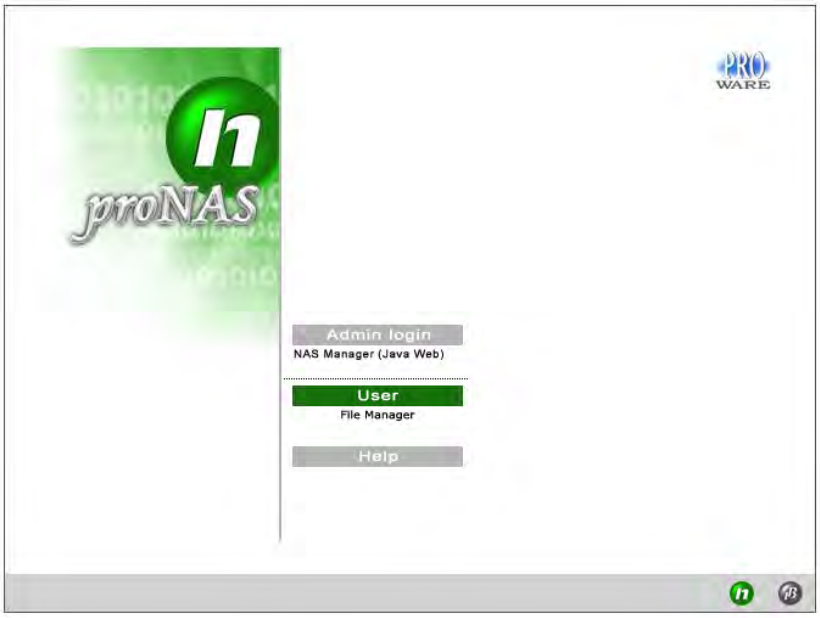
Application	Event	Purpose
pronasha	[proNAS HA] Service Running	Notify if proNAS HA Service is running.
pronasha	[proNAS HA] Cluster Function Running	Notify if proNAS HA Cluster Function is running.
pronasha	[proNAS HA] Cluster Function Stopped	Notify if proNAS HA Cluster Function has stopped.
pronasha	[proNAS HA] Takeover Resource Group Success	Notify if proNAS HA Takeover of Resource Group is successful
pronasha	[proNAS HA] Failover Resource Group Success	Notify if proNAS HA Failover of Resource Group is successful

NOTE: The proNAS HA Application Events appear only when proNAS HA service is running.

Please don't forget to press the **Enter** key after you input the script path.

Chapter 6 File Manager

6.1 Introduction to File Manager



File Manager is a web-base file system for normal account users to do the following actions:

Read a file: User needs the read permission of the folder and the file itself. The file may be opened immediately if the browser knows the corresponding applications that can open it, or the browser will prompt users to save the file in the local computer instead.

Upload a file: User needs the write permission of the folder and the file itself. A browser's upload window will show up and user needs to locate the file from local computer to be uploaded to the current directory.

Create a file: User needs the write permission of the folder. A browser's upload window will show up and user needs to locate the file in local computer.

Delete a file: User needs the write permission of the folder and the file itself.

Rename a file: Same as above. User needs to give the new name of a file.

Change Password: If user needs to change password, please select this function.

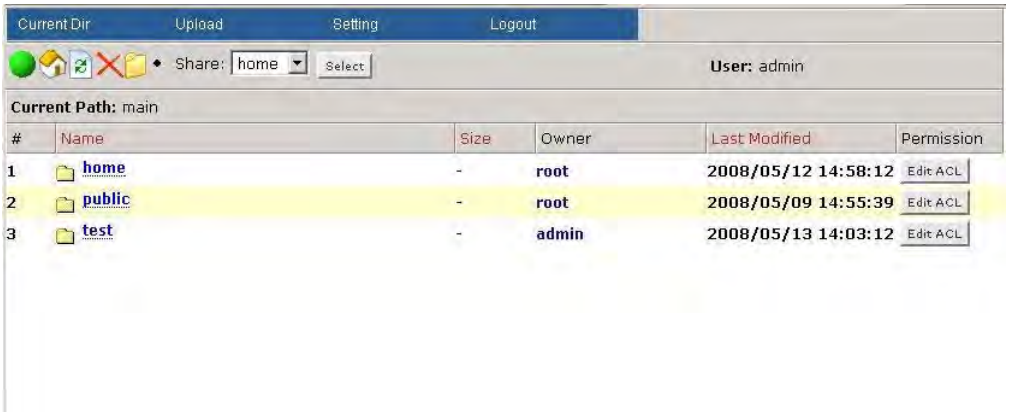
Access Right (Change the ACL of a file or sub-folder): User needs to be the creator or the owner of the share folder. A user is the creator of a file or folder if user creates it. The owner of a share folder can grant the access permission of a share to other accounts or access groups. User also can manage the ACL of all the files and sub-folders under the share.
The function of access right is for share owner to do more detail management for the users accessing the shares. Share owner can increase or delete the access right of users or groups in addition to the setting of administrator in proNAS GUI. Furthermore, share owner can manage the detail access right of the subfolders.

6.2 Logon to File Manager

NOTE: Make sure the "File Manager server" is started (status is Running) in System Manager -> Service.

Enter the username and password to pass authentication.

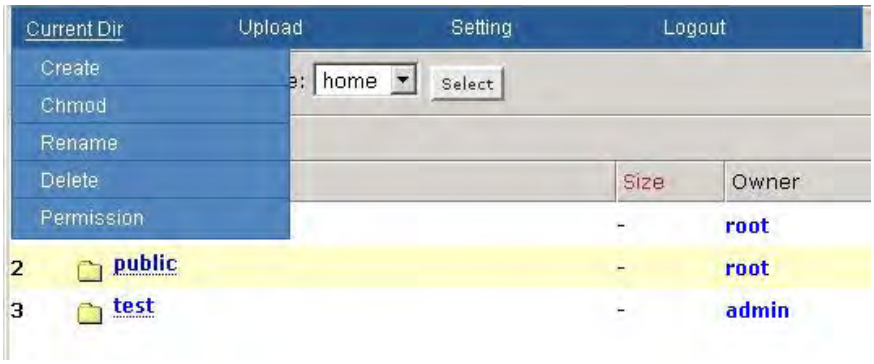
The first Screen of file Manager will display and help users to understand the possible options and to perform file management. There are 4 Main Menu in the File Manager screen: CurrentDir, Upload, Setting, and Logout. There are also short-cut icons below the main menu, like Main, Home, Reload Page, Delete Current Folder, and Create New Folder.



6.3 Directory and Upload Function

NOTE: Operations in the main Share folder, such as changing ACL or deleting the share itself, is not permitted. This must be done in Share Manager in proNAS GUI.

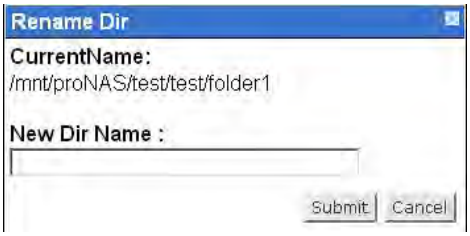
Current Dir – Shows possible options that can be done in the current directory.



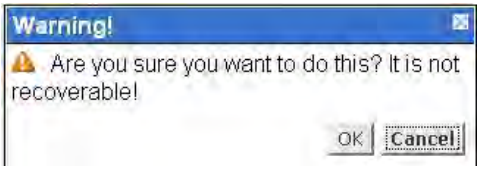
- Create – Allows user to create a new directory.

- Chmod – Allows user to change the file access permission on the current directory.

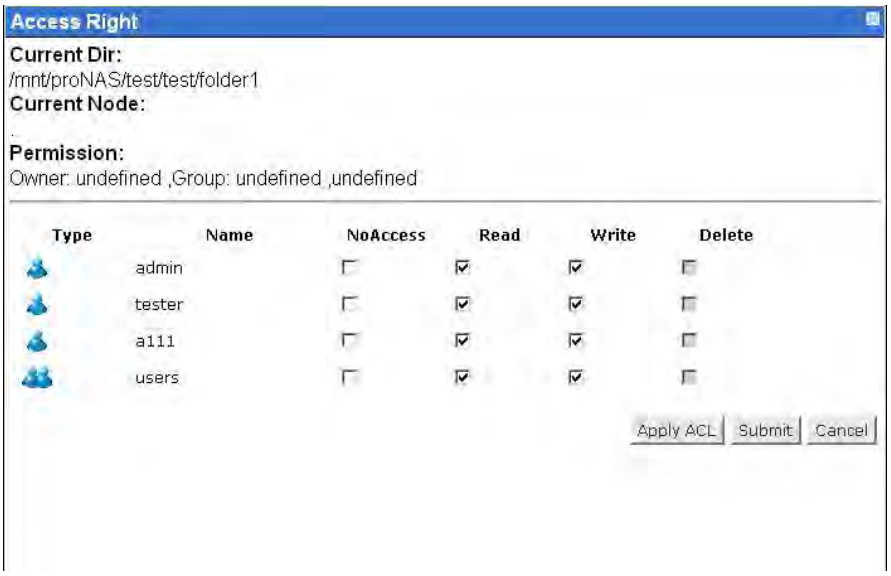
- Rename – Allows user to rename the current directory.



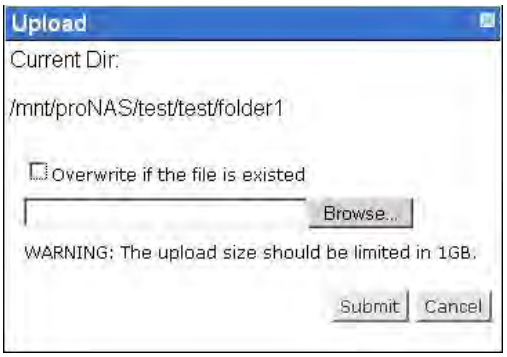
- Delete – Allows a user to delete the current directory.



- Permission – Allows user to change the Access Rights of different users on the current directory.



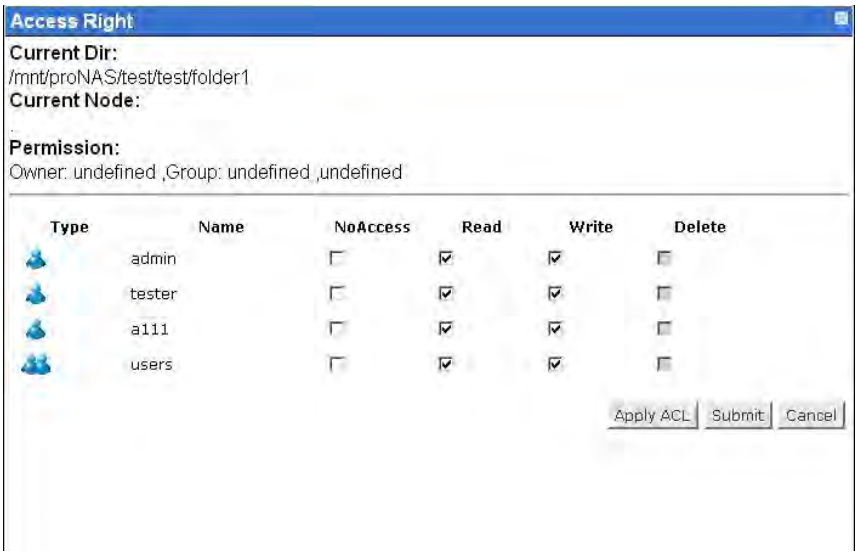
Upload – An option used to upload a local file into the current directory. Use the "Browse" button then select the file to upload.



WARNING! The file size to upload should not be greater than 1GB.

6.4 User Access Right and Group Access Right

A user who is the owner of the share can grant access permissions to other users or groups listed in the Permission list.



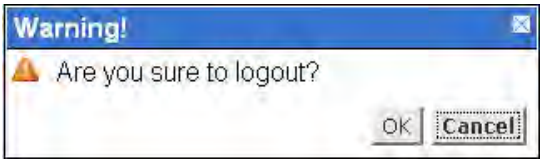
After changing the Access Rights, click the “Submit” button. The ACL will be saved and updated only in the current directory or sub-folder. To update other directories or sub-folders below the current directory, use the “Apply ACL” button. This will propagate the current ACL to the ACL off all files and sub-folders below. To cancel any changes, click the “Cancel” button.

6.5 Change Password and Logout

Setting – Allows a use to change his/her password.

NOTE: The password must be at least 6 characters in length.

Logout - Allows a user to logout from the current session of File Manager.



Chapter 7 proBackup

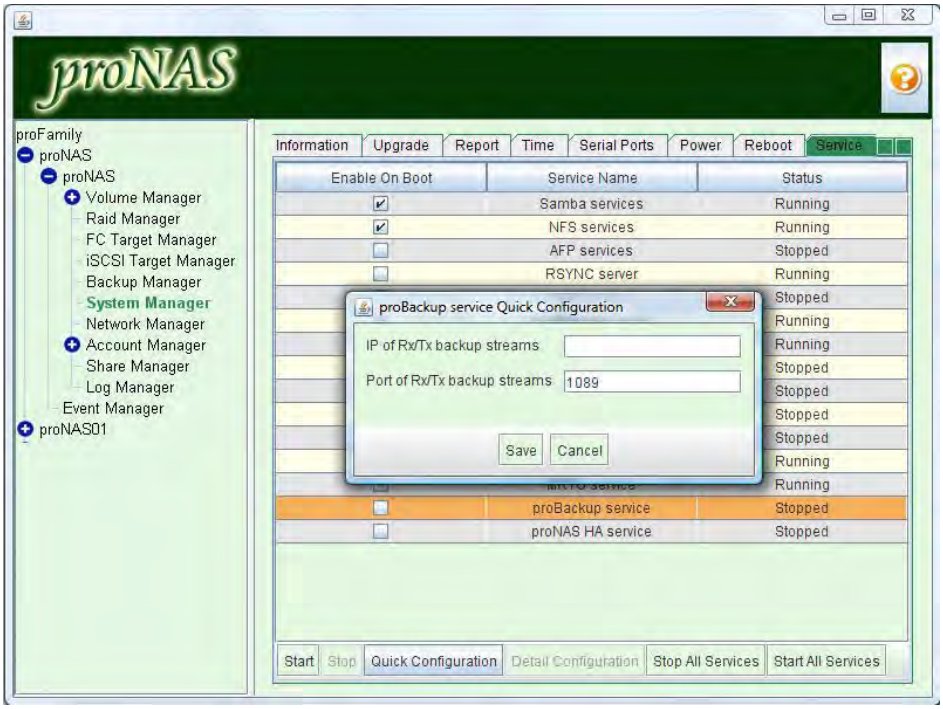
7.1 Introduction to proBackup

proBackup provides end users a friendly Java GUI that makes versatile backup functions available to general users. They can easily backup and restore their files to and from proBackup storage device, and they do not need to install proprietary software in their machines. It is also simple to setup a proBackup storage for a company or an organization, even for non-IT-pro person.

7.2 Administrator Logon

The administrator account, admin, can login to proBackup. In proNAS Manager, admin can also assign other privileged users to become member of the proBackup group. Only admin and members of the proBackup group can login to proBackup and perform proBackup functions.

Before admin or proBackup user can login to proBackup Java GUI, the proBackup service must be started in Service tab of System Manager. In Quick Configuration, setup the "**IP of Rx/Tx backup streams**" to the **proNAS IP address** that will be used as the channel for proBackup. The "**Port of Rx/Tx backup streams**" is set to 1089 by default. If this port is already used, assign another port.



After setting the Quick Configuration options, start the proBackup service. When the proBackup service is in “Running” status, login to proBackup Java GUI can be done. The default Logical Volumes **proBackup Device** and **proBackup Extended Device** will also be created.

To login to proBackup java GUI, open web browser then type the proNAS IP address.
Click the proBackup icon on the lower right side of the page.

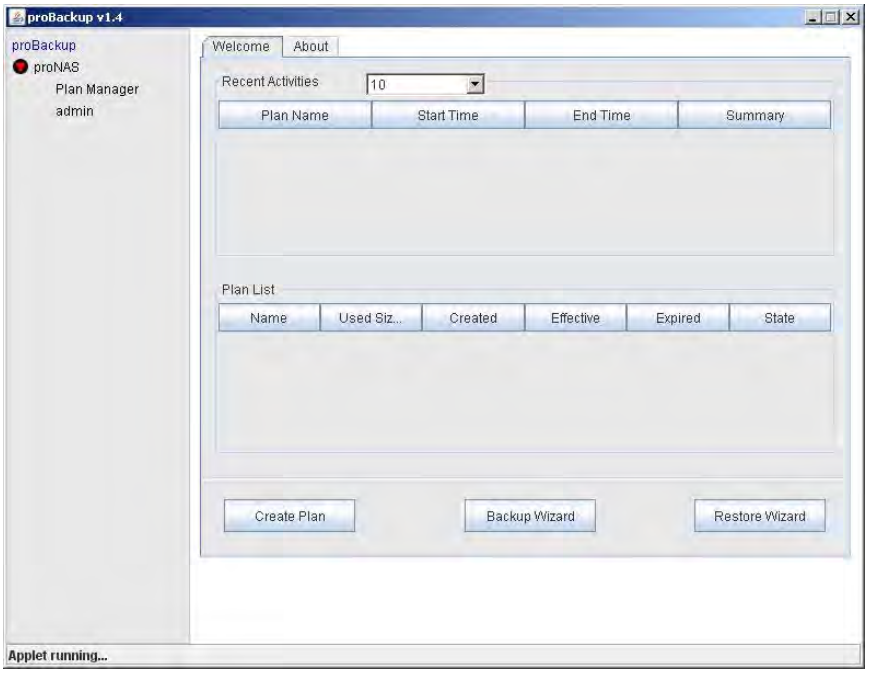
The proBackup page will be displayed. Click “Start Java Web”.

Enter the login account and password.

NOTE: All the backups of an account are lost forever if it is deleted. Please make sure of such action before doing it.

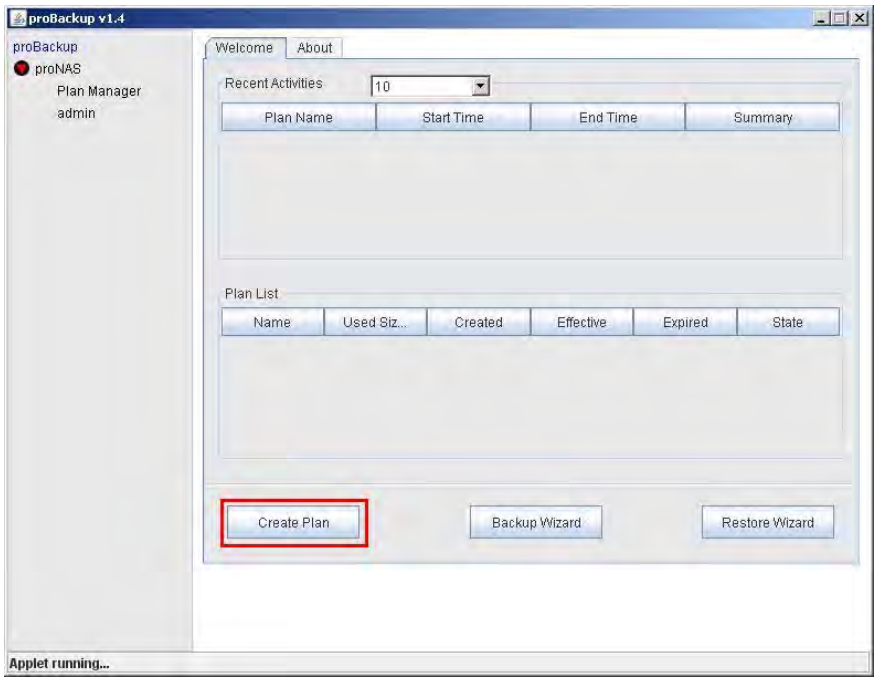
NOTE: It is advised that only the organization privilege persons can assume the role of administrator since it can restore all others' data, which may contain sensitive information.

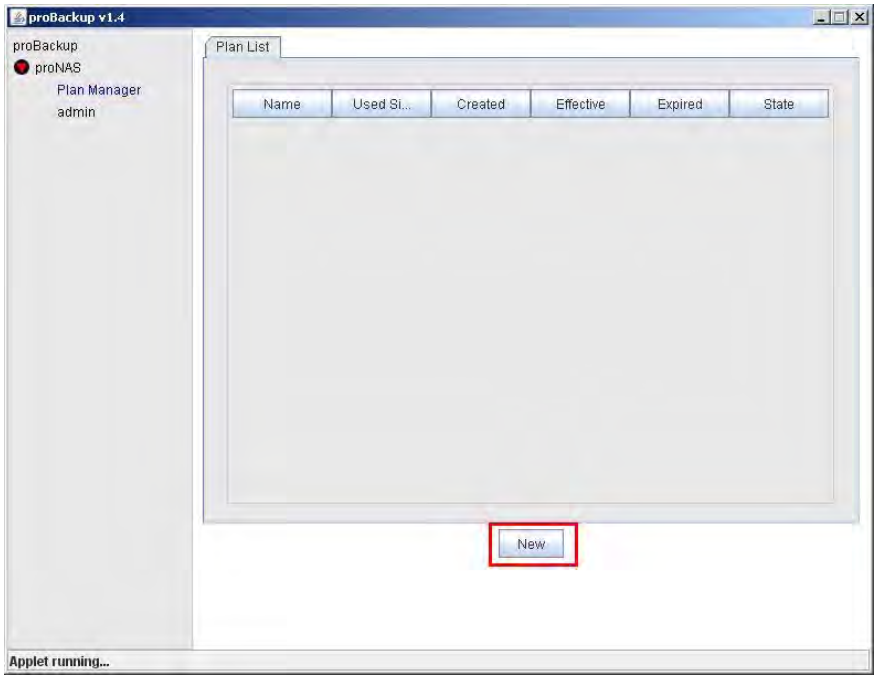
The proBackup Java GUI Welcome screen will be displayed. You can view the recent proBackup operations and existing backup plans in the Welcome screen. To learn about proBackup release version, click the About tab.



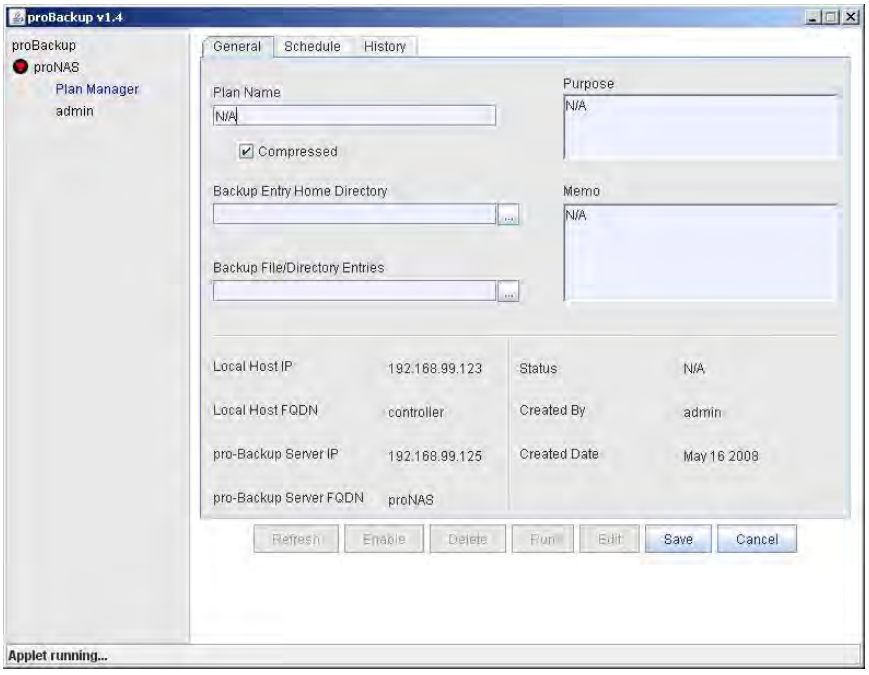
7.3 Create Backup Plan

To create backup plan, either click the “Create Plan” button in the proBackup main screen or click the “New” button in Plan Manager.



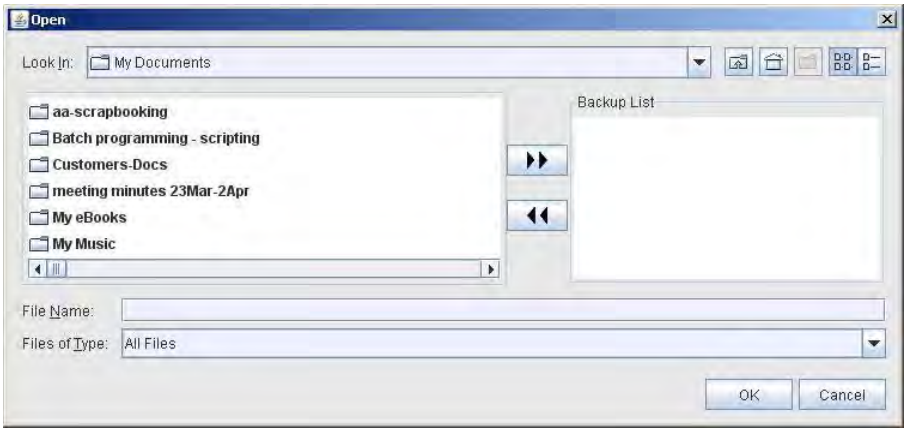


The General tab of Plan Manager will be displayed. Fill in the required fields. Some information about Local Host and proBackup Server are also shown.



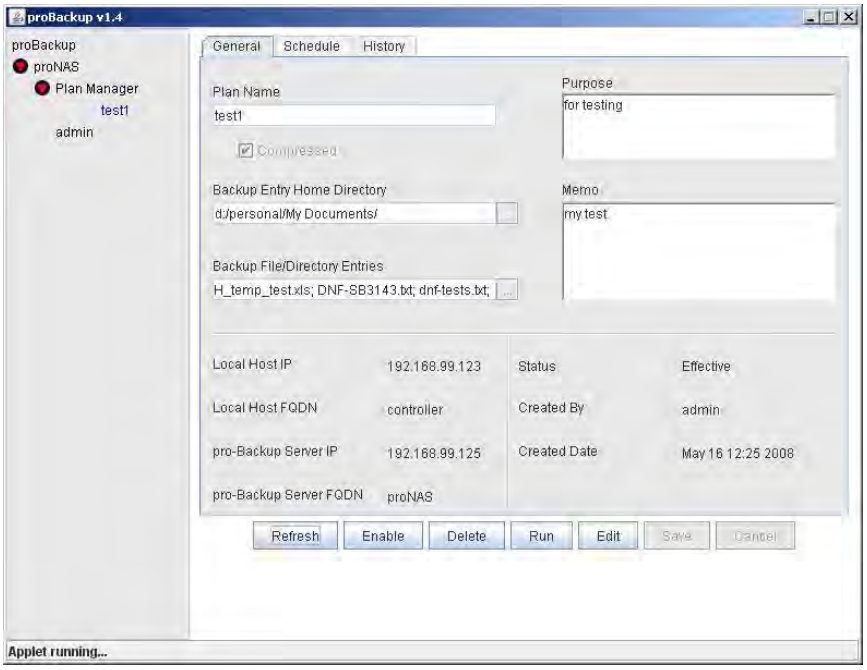
The Configuration options:

- **Plane Name** – Enter the backup plan name.
- **Compressed** – If checked, the backup will be in compressed format.
- **Backup Entry Home Directory** – Click the "…" button then select the directory when data will be backed up.
- **Backup File/Directory Entries** – Click the "…" button. Select the files and/or directories to be backed up then click ">>" button to add them to the backup list. Click "OK" to go back to General tab.



- **Purpose** – Enter additional information in this optional field.
- **Memo** – Enter additional information in this optional field.

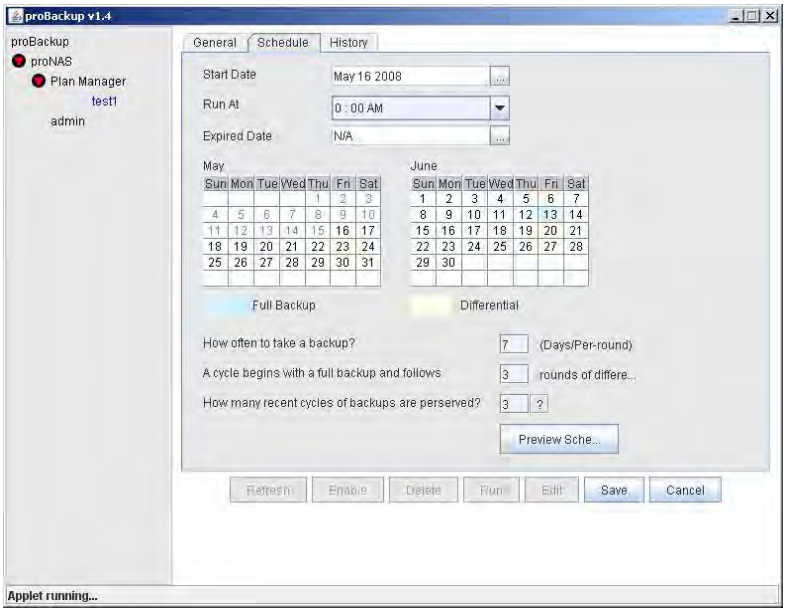
After completing the necessary information, click “Save” button. The Backup Plan will be saved.



Function buttons in the General tab.

- **Refresh** – Refresh the information about the current backup plan.
- **Enable** – Activates the backup plan schedule. When enabled, a “**Disable**” button will appear which can be used to deactivate the backup schedule.
- **Delete** – Deletes the current backup plan.
- **Run** – Execute the backup plan immediately.
- **Edit** – Use this to change settings in the backup plan.

To add schedule in the Backup Plan, click the “Edit” button then select Schedule tab. Configure the Schedule options then click “Save” when done.



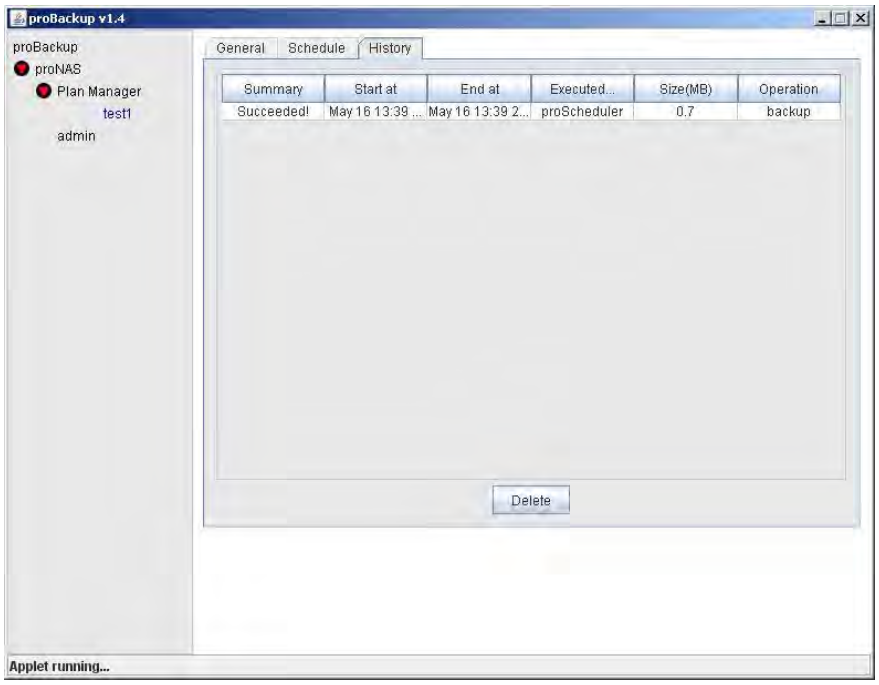
Schedule options:

- **Start Date** – The starting date when the backup will be done. This usually defaults to the current date. Click the “…” button. A calendar will be displayed. To change the Start Date, select a new date in the calendar.
- **Run At** – The preferred time to run the backup. To change the Run At time, click the pull-down arrow then select the preferred time.
- **Expired Date** – The ending date for the backup. To change the Expired Date, click the “…” button then select in the calendar the preferred last date of backup.
- **How often to take a backup? (Days/Round)** – The number of days that will pass before a differential backup will be done.
- **A cycle begins with a full backup and follows rounds of differential backup** – Enter the number of differential backups that will be made before starting a new full backup.
- **How many recent cycles of backups are preserved?** – Enter a number which is the total number of backup cycles that will be preserved. A backup cycle starts with a full backup and ends with the last differential backup before the next full backup. When the number of cycles in a schedule has been reached and a new cycle is started, the oldest backup cycle will be automatically removed.
- **Preview Schedule** – Click this button to update the calendar schedule.

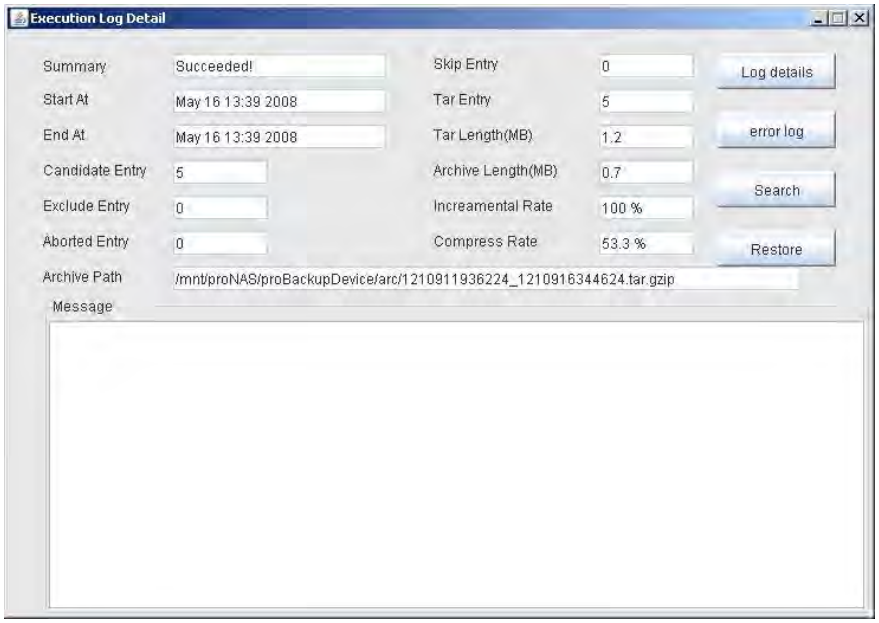
    - **Full Backup** – archival backup; all files are copied to a backup storage device
    - **Differential Backup** – backup only the data files that have been modified since the last full backup

Click “Save” to update the schedule settings. Then click “Enable” to activate the backup schedule.

The History tab shows a log or list of operations that have happened in proBackup such as backup or restore operation. To delete an entry in the history list, select the item in the list and click “Delete”.

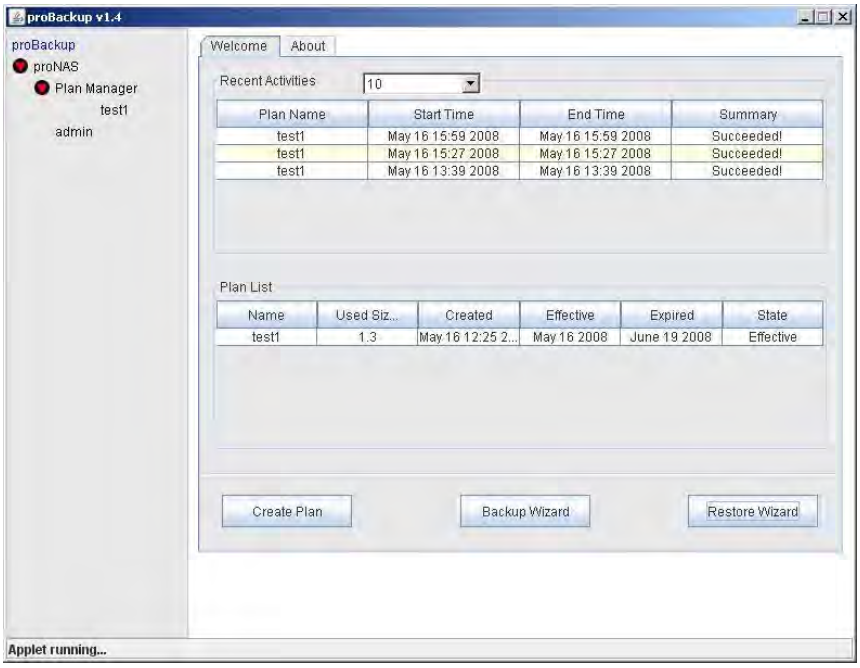


To view detailed information about the backup, double-click the item from the History tab.



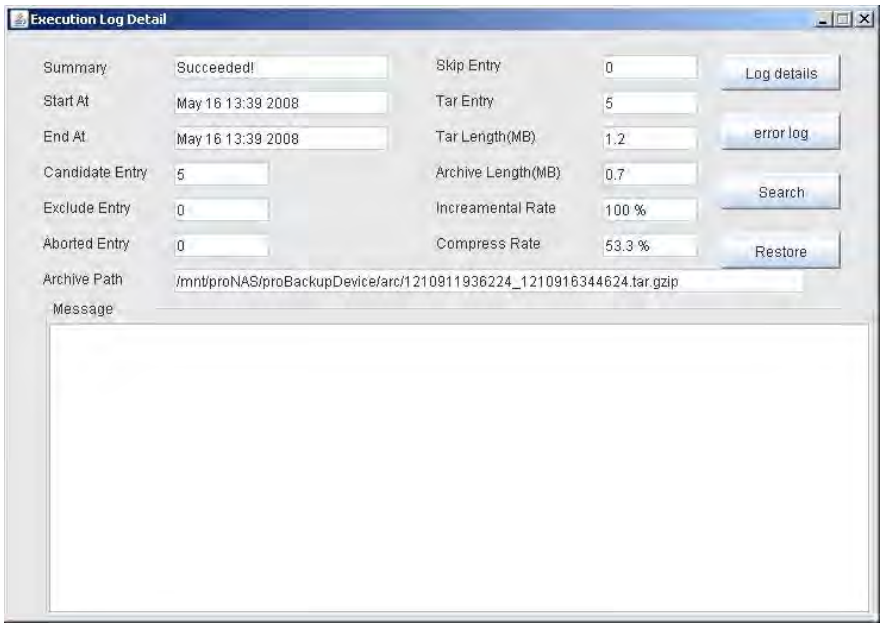
“Log details” is used to display detailed information about the execution process.
“Error log” will display errors that happened during the execution process.
“Search” will allow you to search for a string currently displayed in the Message screen.
“Restore” will allow you to restore a backup.

Another alternative to do backup or restore is to use the Backup Wizard and the Restore Wizard. Click proBackup in the left tree node. The Welcome screen will be displayed where the Backup Wizard and Restore Wizard can be used.



7.4 Restore Backup

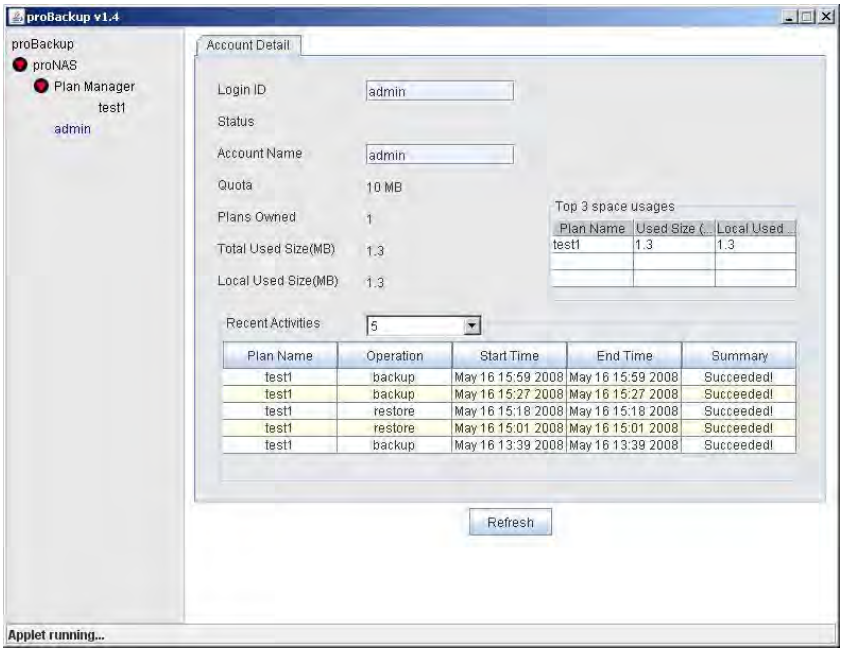
To restore a backup, double-click the backup item from the History tab. The Execution Log Detail window will appear.



Click “Restore”. Then input the destination where the data will be restored. Or click the “Browse” button then select the destination directory or folder where data will be restored. Click “Ok” to start the restore process.

7.5 Account Detail

Under Plan Manager, click the account name to view information about the account.



Chapter 8 proNAS HA (Optional Function)

8.1 Introduction to proNAS HA

proNAS HA (High Availability) provides solution for business continuity with automatic failover which ensures that should a critical server become unavailable - due to failure or maintenance-related downtime — a replica will immediately provide all services in its place without the need for time-consuming manual procedures.

The core processes of ProNAS HA are implemented as two mutual-guarded fail-safe proNAS services. They can be manipulated by accessing the Services tab in the proNAS System Manager node. The dual service architecture of ProNAS HA prevents ProNAS HA from being the single-point-of-failure of the server cluster.

When a server is down or unavailable, ProNAS HA switches the critical operations of that server over to the peer server automatically. The switch over procedure can also be triggered manually to handle scheduled downtime more gracefully and user transparently. ProNAS HA can be manually instructed to switch over the critical operations of a server to the peer server. Users can then perform upgrade, replacement, or maintenance to the hardware and software of that proNAS server. The critical operations of a server can be configured as auto-switch back. After those critical operations were taken over by the peer server, ProNAS HA can switch them back to their original active server when the active server becomes available again. Auto-switch back ensures that the original load distribution between the two servers will be resumed immediately when possible.

proNAS HA provides:

- Manual or auto-triggered failover to a standby server.
- Supports manual or automatic failover back to the original server when ready
- Real-time replication minimizes potential data loss

NOTE: proNAS version 1.3.xx supports Replication of Logical Volumes with LV capacity up to 16TB. proNAS HA also has the same LV size limit, which means all logical volumes in proNAS (under HA) must not exceed 16TB.

8.2 Getting Started with proNAS HA

Before Configuring High Availability

Before attempting to configure two proNAS servers as a High Availability pair, check the following requirements:

1. **Each proNAS server node must have a different and unique hostname. (It is highly recommended to use the same NAS model.)**
2. **Each proNAS node must have at least two static IP addresses.**
3. **Must have a reliable heartbeat, private net Ethernet is required, serial RS232 is optional.**
4. **ProNAS HA services must be started in both proNAS servers.**
5. **The maximum number of logical volumes that can be created under HA is 32.**
6. **ProNAS HA does not support logical volumes larger than 16TB. Users can create and extend volumes larger than 16TB but this cannot be used in proNAS HA.**
7. **Changing hostname and IP addresses when proNAS HA is running is not allowed.**
8. **Snapshot function is disabled under HA.**
9. **Be sure there are no scheduled snapshot task enabled either on each proNAS box.**
10. **ProNAS HA service cannot be started if iSCSI volume exists, Replication is running, or snapshots exist. Make sure to remove all iSCSI volumes, stop Replication, or delete snapshots.**

Setting up a private network:

Private net is a communication channel between the two proNAS box through which they exchange information about their states (*heartbeats*). proNAS supports two private network, TCP/IP Socket and RS232 Serial Port.
To setup TCP/IP private net: Connect a dedicated network into Ethernet1 adapter. You may use a crossover cable. Ethernet0 serves as your public net.
To setup RS232 Serial Port private net: Connect a serial cable to either Com1 or Com2 of both proNAS nodes then configure it under the "Serial Port" tab on System Manager.

NOTE: It is recommended to use both TCP/IP and RS-232 for your private net. Private net IP will be used for replication and RS-232 for heartbeat.

NOTE: You can setup LAN0 Gigabit port (eth0) as your public net; that is where the users access your proNAS, and also for accessing proNAS management GUI. Then use LAN1 (eth1) as your Private Net.

8.2.1 Hardware Aspect

Active server: proNAS HA server that performs cluster-protected operations.

Backup (Standby) server: proNAS HA server that can takeover the critical operations of an active server when the active server is down or unavailable.

Private net: Private net is a dedicated channel for servers to exchange their operating status (i.e., heartbeat message).

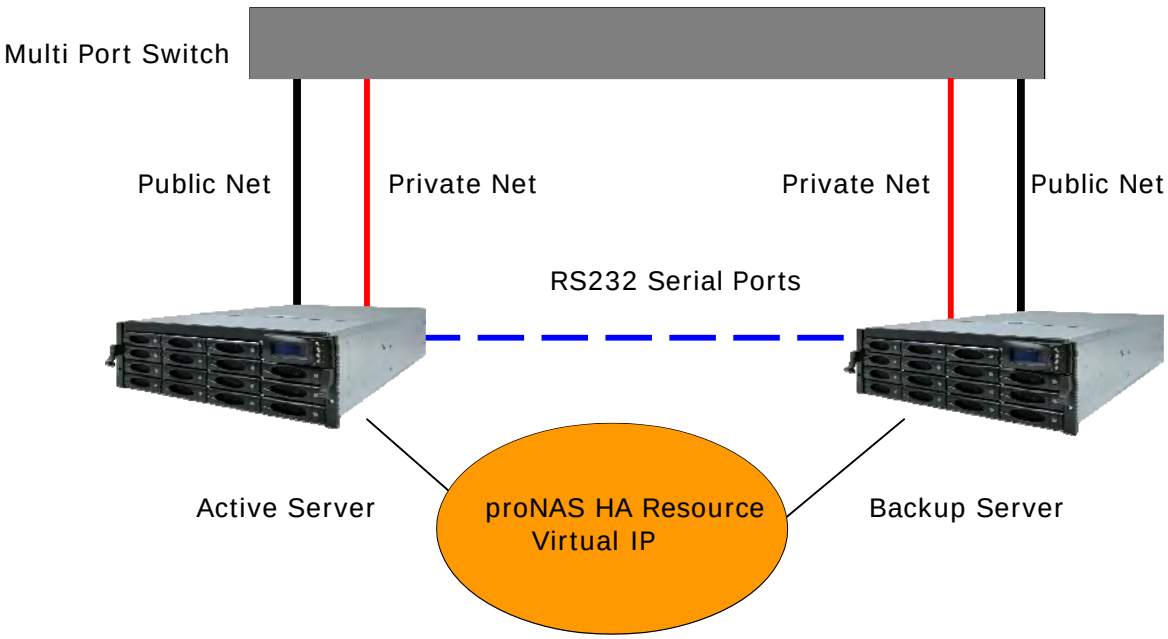
Types of Private Net Available:

- **TCP / IP socket:** Ethernet network running TCP/IP protocol. Each server must install a dedicated IP to attach to the private net.
- **RS-232 serial port:** One free serial port per server. A null modem cable must be installed to connect the serial ports of the two servers.

Public net: Public net is the paths for networked clients to access cluster- protected resources.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a High Availability pair:



8.2.2 Procedure for Setting Up proNAS HA

Setting up a server cluster:
Below are the basic steps in setting up a server cluster:

1. Configure the hostname for both proNAS servers (must be unique).
2. Configure two static IP addresses for each proNAS server.
3. Set up private net. At least the private net IP must be configured to start cluster.
4. Start proNAS HA service for both proNAS servers. You may do this under System Manager then Services tab, highlight proNAS HA service then click Start. proNAS HA node will then appear on the left tree after it starts successfully.
5. On the designated Active Server, go to proNAS HA->"General Settings".
6. On the "General Setting" tab, click "Edit" button. Input the Peer Server hostname then select "**Active (local-host) – Standby (peer host) Mode**" under the Cluster mode. Click "Save".

NOTE: The Cluster Mode of Backup Server must be configured as "Standby(local host) – Active(peer-host) Mode" (see Step 10).

Other configuration options:

Computer Name:

Local Server: The hostname of the Active or Primary server
Peer Server: The hostname of the Backup or Secondary server

Reference IP:

Enable Reference IP Checking – Select this option to enable reference IP checking. A Reference IP is an IP address that the proNAS HA service will check when the heartbeat channel(s) between the two servers are lost. This IP will be used as a reference point to device whether the network really has a problem before doing failover or takeover. HA will ping the local and virtual IP address of proNAS, and for any reason that this fails, HA will ping this reference IP as a double check. If ping still fails, proNAS HA will proceed with failover or takeover. The IP of a router or any network device which is always online can be used as a Reference IP.

IP Address – Enter the IP address of the Reference IP to check the availability of the servers.

Event Log:

Level – Select the type of logging that will be used for proNAS HA service. Default is Normal which shows operation processes. Other option is Trace, which shows operation and traceable processes.

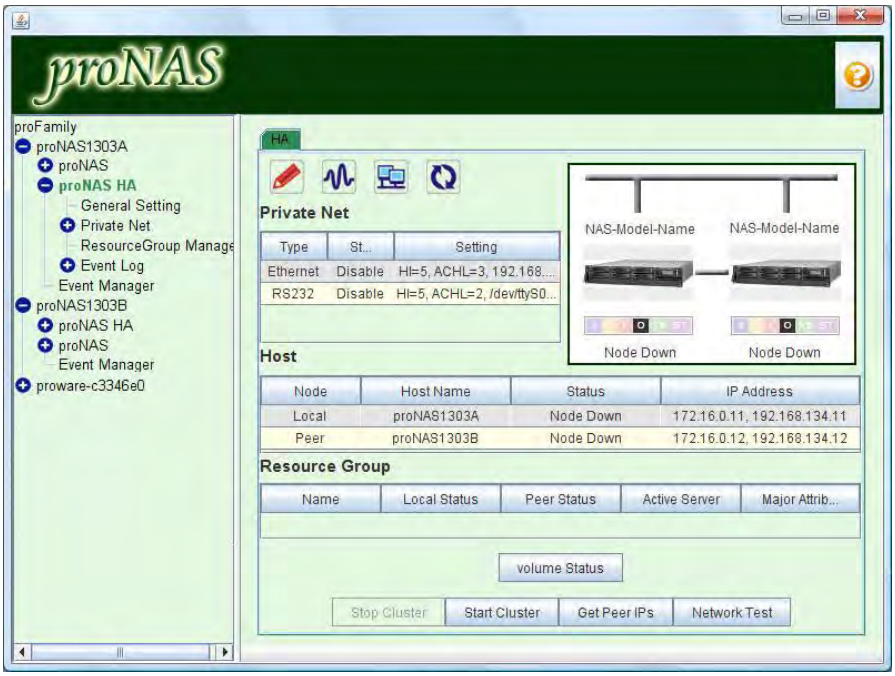
Preserved Days – Select the number of days that the log will be preserved before deleting.

Operational Preferences:

On Server Shutdown, failover the resource groups automatically – When enabled, the resource groups will be failed over to the other server when this server shutdown.

On Server Startup, start the cluster system automatically – When enabled, the cluster system will be started automatically when this server starts up.

7. Back to proNAS HA node, click "Get Peer IPs" button. The IP addresses of the peer server will then be displayed in the status info table. Be sure that it gets the peer IP addresses! If it fails, check again the hostname that you supplied in step 6.

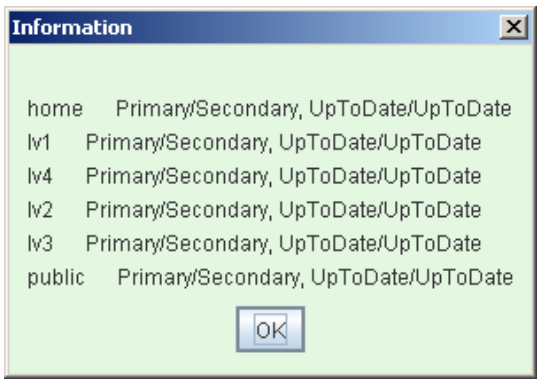


Buttons:

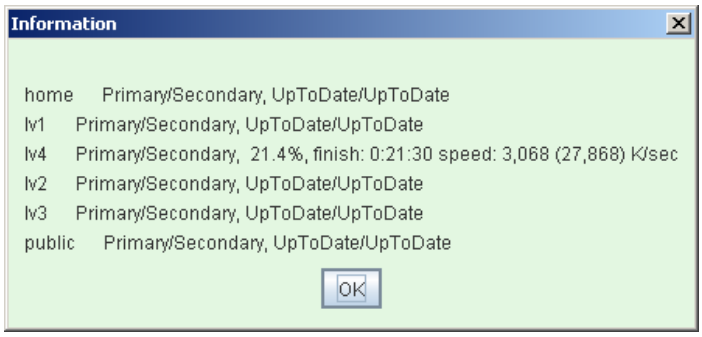
Stop Cluster	Stop Cluster Operation.
Start Cluster	Start Cluster Operation.
Get peer IPs	Get the IP's of the peer server and display it in the host peer table.
Network Test	Tool for testing network IP address (e.g ping ip)
Volume Status	Shows the current Replication status of logical volumes.

NOTE: When HA is already configured and Cluster is in operation, you can see the current replication status of logical volumes by clicking "Volume Status".

Volume Status Example 1: All logical volume Replications are up to date.



Volume Status Example 2: Replication of one logical volume is initializing.



8. Go to Private Net node down to "Ethernet#1". Set the local and peer IP address, check "Auto Enable on Starting Cluster" then save. Be sure not to select the public IP (eth0 IP address) for both proNAS servers.

Private Net: Ethernet

Local/peer Port Number	Specify an unused TCP port for each server to receive the heartbeat sent from the peer server. The default value is 5000.
Local/peer IP Address	Specify the IP Addresses of the network interface cards that constitutes both ends of the private net. These IP addresses must be on a separate subnet from the public net.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.

Acceptable Consecutive Heartbeat Loses	Each server will keep counting and timing the heartbeats received from the peer server. If the number of times a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically when starting cluster. Add the checkmark to enable this option.

9. Configure private net "RS232#1", if you setup serial port as an additional private net.

Private Net: RS232

To use RS232 as a private net, you need to configure Serial ports settings in proNAS System Manager > Serial Ports tab, select either COM1 or COM2 for proNAS-HA.

Local Serial Port	Specify an unused serial port for each server to receive the heartbeat sent from the peer server.
Baud Rate	Specify the Baud Rate of the selected serial ports.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.
Acceptable Consecutive Heartbeat Loses	Each server will keep counting and timing the heartbeats received from the peer server. If the numbers of times a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource groups of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically on starting cluster. Users can add the checkmark to enable this option

10. Follow the same steps from step 5 to step 9 to configure your standby Backup Server except you need to select "**Standby(local host) – Active(peer-host) Mode**" as the Cluster Mode.

11. Click "Start Cluster" button.

12. Wait until the status of the local and peer server are in be standby-standby mode respectively. The statuses of the private net must also be "Enabled and Healthy". If this is not the output, check and repeat previous steps.

13. Go to "Resource Group Manager" then press "Add Resource Group".

The Resource Group Manager of proNAS HA is used to manage resource groups. Users need to configure resource groups only on one of the servers, usually the Active server. proNAS HA will automatically synchronize the status of resource groups between both servers. Note that users are prohibited to create or remove resource groups unless proNAS HA are running on both servers and at least one of the private net is functioning.

Buttons:

Add Resource Group button	Add new resource group member. User can specify the name of the resource group. This name must be unique for the resource groups within the cluster
Switch All Resource Groups from Peer	This is to manually takeover the all resource groups from the peer server. Users can manually takeover resource groups from the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.
Switch All Resource Groups to Peer	This is to manually failover the all resource groups to the peer server. Users can manually failover resource groups to the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.

14. Input a resource group name. You may check "Auto Switch back" or "Auto Bring In" then click “Save”.

Resource Group Properties:

Resource Name	A unique name for identifying the resource group
Active Server	The active server of the resource group
Backup Server	The peer server is automatically display
Local Status	The status of the local server
Peer Status	The status of the peer server
Auto-switch back	An option for enabling the Group to be switched back from the Backup server to the Target server automatically when the Target Server is available again.
Auto Bring In	An option for enabling the resource group to be brought in automatically when Cluster is started.

Buttons:

Bring in	The selected resource group will be activated and brought under the protection of proNAS HA. This button is only visible if there are resource group added.
Bring out	The selected resource group will be brought out from the protection of proNAS HA. A resource group can be brought out of cluster to perform maintenance or troubleshooting. This button is visible if resource groups are brought in.

15. Click the resource group name on the left tree node then press "Add Resource".

16. On the "Basic Settings" tab, input a resource name.

Resource Basic Setting:

Resource Name	A unique name for identifying the resource group.
AC interval (Availability Check Interval)	A time interval for proNAS HA to check the availability of the resource group periodically.
AC Retry (Availability Check Retry)	The number of times for proNAS HA to check the availability of the resource group periodically.
Stop timeout	Specify the period of time for resource startup and stop. If a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Skippable if releasing resource fail	This option is disabled by default. Basically all of the resource group of the peer server will be taken over when the peer server fails. Users can add the checkmark to enable this option. The failover will be taken even if resource releases fail.

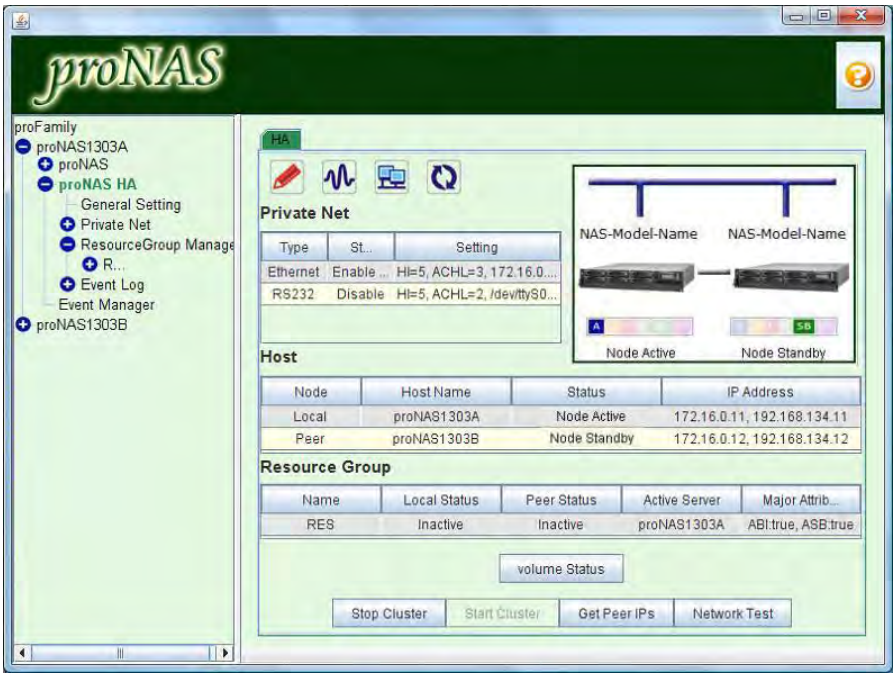
17. On the "IP Address Resource" tab, select the original IP address (eth0 IP) for both local and remote proNAS, enter an active IP address, active subnet mask and then save. Active IP address is the virtual IP address.

IP Resource:

Original IP Address	Choose the original IP Address for the local and peer server.
Active IP Address	Type an IP Address (virtual IP) for client-end applications to access specific resources on the NAS Target Server.
Active Subnet Mask	The subnet mask used by the Active IP Address.

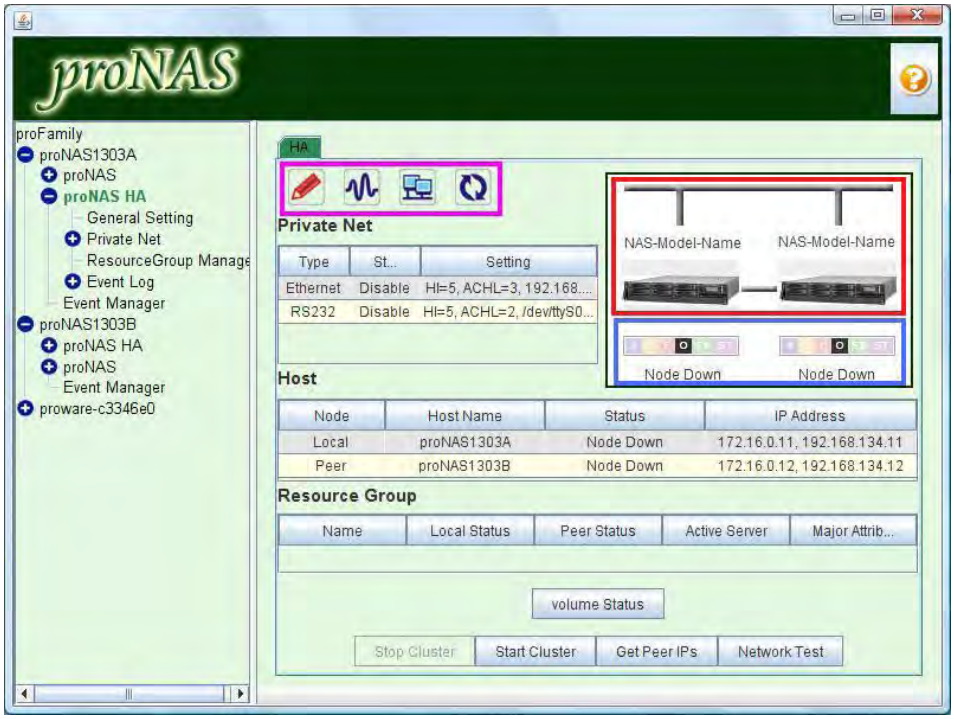
18. Click the resource group name on the left tree node then press "Bring In". The resource name will be brought in.

19. The Cluster Servers will be in Active – Standby mode.



8.3 ProNAS HA Properties

Status Properties



Users can monitor all the resources from the proNAS HA Status Pad. Users can monitor the status of the servers, the resource groups and the private net in real-time. The status after the Cluster Service starts running on both servers.

The status icons in status bar and their respective meaning:

- Active Mode

- Error Mode

- Fail Mode

- Offline Mode

- Standby Mode

- Startup Mode

The private net status:

The colored lines between the servers indicate the status of the private net. Also status is displayed in the function bar.

- **Gray line** Only one end of the Private Net is created, the other end is not yet created.
- **Red line** Both ends of the Private Net are established but either one of the servers can not receive heartbeat message from the peer server.
- **Blue line** Both ends of the Private Net are established and both servers are exchanging heartbeat messages.

Indicators:

Users can accurately monitor the status of the system such as the License status, Private Net, Public Net and the resource takeover/failover. When a condition occurs, the icon will turn red. You will also see a message appear in the Event Log.

Private Net: This icon will turn red if there's a problem with the connection of the private net.

Public Net: This icon will turn red if there's a problem with the connection of the public net.

Failover/Takeover: This icon will turn red during the failover or takeover scenario.

License: This icon will turn red if proNAS HA is not registered.

Host box: Display the status of Local and Peer Server

Resource Group box: Display the resource group status

Buttons:

Stop Cluster button	Stop Cluster Operation.
Start Cluster button	Start Cluster Operation.
Get peer IPs button	Get the IP's of the peer server and display it in the host peer table.
Network test button	Tool for testing network IP address (e.g ping ip)

8.4 Extending a Logical Volume in HA

Extending a logical volume while in cluster is basically not allowed same as in replication, however here is the workaround.

1. Stop Cluster
2. Stop HA service for both proNAS.
3. Abort the replication of the logical volume that needs to be extended.
4. Extend the logical volume on the Active server.
5. Removed the logical volume (the replica) on the standby server.
6. Start HA service for both proNAS.
7. Start cluster.

NOTE: The extended LV size must not exceed 16TB.

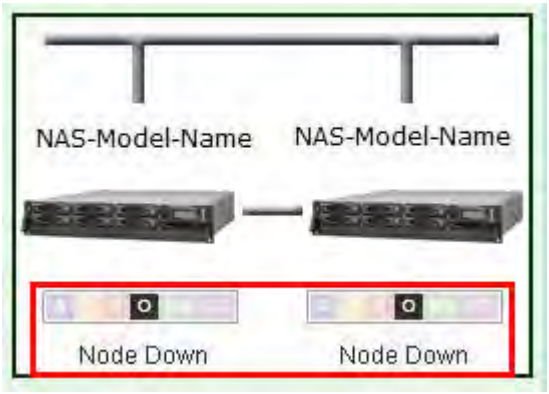
8.5 Clear All HA Configuration

A function button “Clear All HA Configuration” is provided to remove all proNAS HA configuration. This is located in General Setting tab.

When you clear the HA configuration, you have an option to clear all logical volume Replication. If you don’t clear the all Replication, only HA configuration will be reset, and all logical volumes will still have Replication.

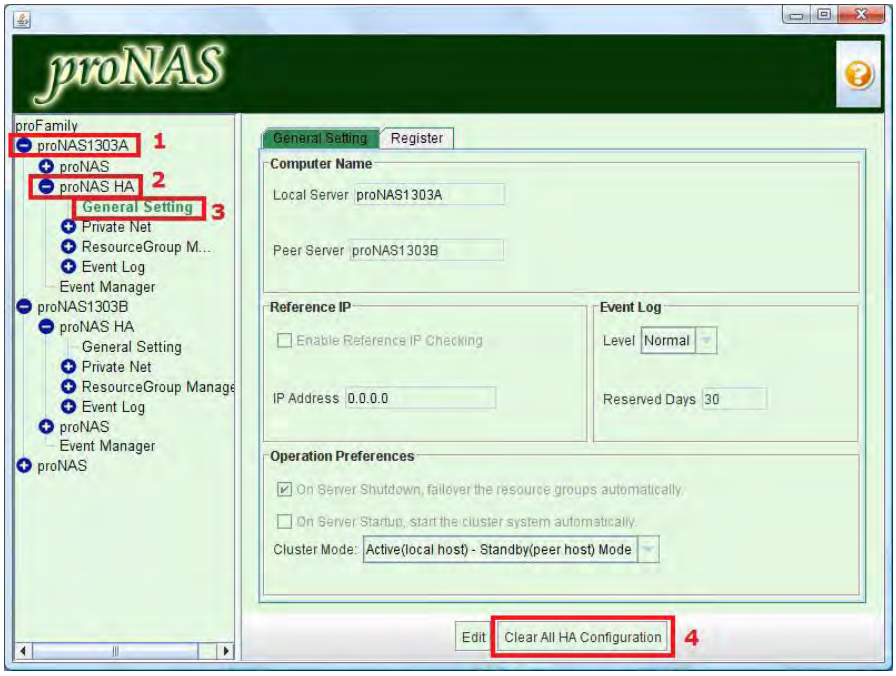
After you clear all HA configuration and clear all Replication, you can re-configure another HA. This is normally used when one of the proNAS servers has failed and you want to reconfigure HA for another (new) proNAS server using the remaining proNAS server.

IMPORTANT: Before you clear all HA configuration, make sure the cluster is stopped (all nodes are “down”).

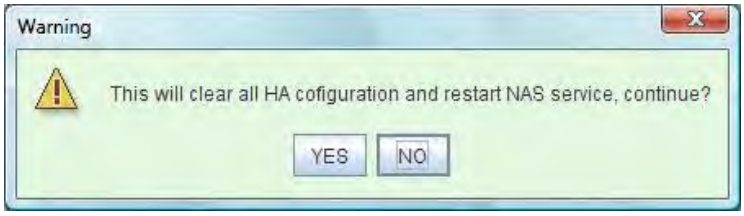


To remove all existing proNAS HA configuration:

1. Select the proNAS node name, click proNAS HA, and select General Setting. Click “Clear All HA Configuration”.

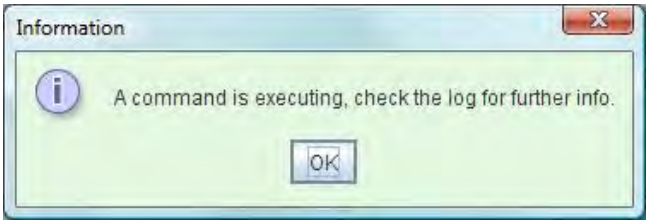


2. A warning message to clear all HA configuration will be displayed. Click “Yes” to proceed.

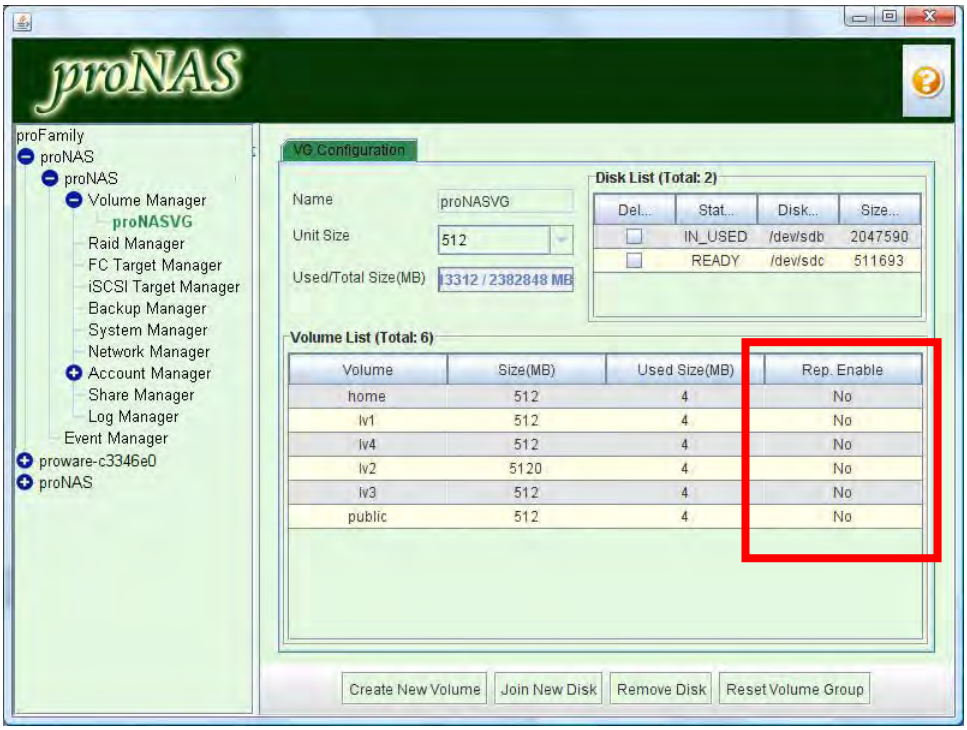


3. A warning message to remove all replication in logical volumes will be displayed. Click “**Yes**” to **remove Replication** in all logical volumes, or “**No**” to **just clear HA** but **Replication of logical volumes still exists**.

4. An information message will be displayed. Click “OK” to close the message. You can verify the proNAS HA Event Log for further information.

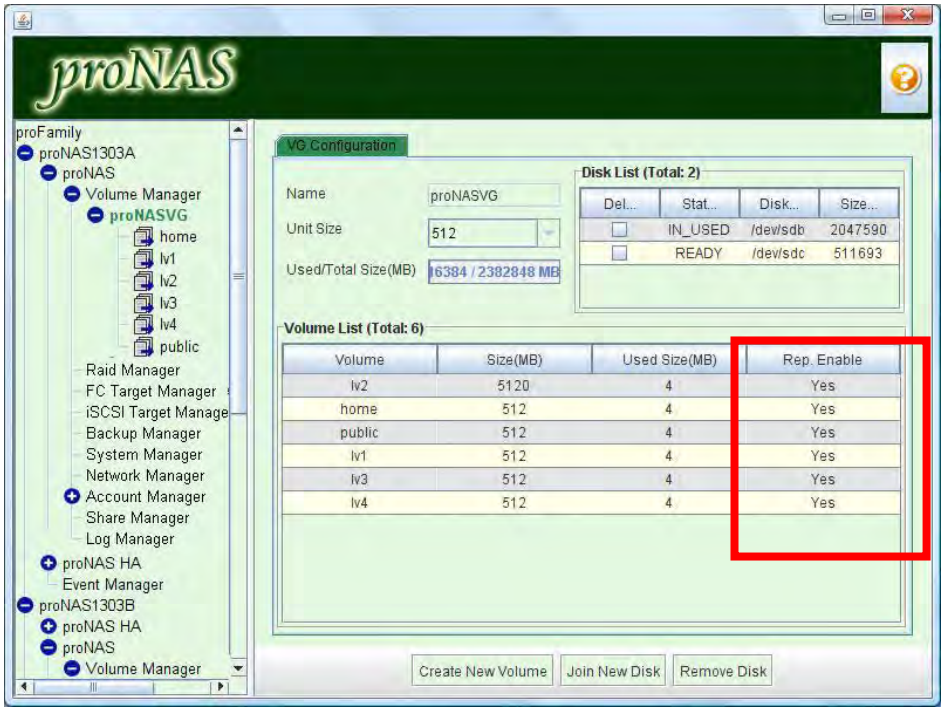


Example of Replication Status after selecting "**Yes**" to remove all Replication:



All Logical Volume Replication are disabled (Rep. Enable shows "No")

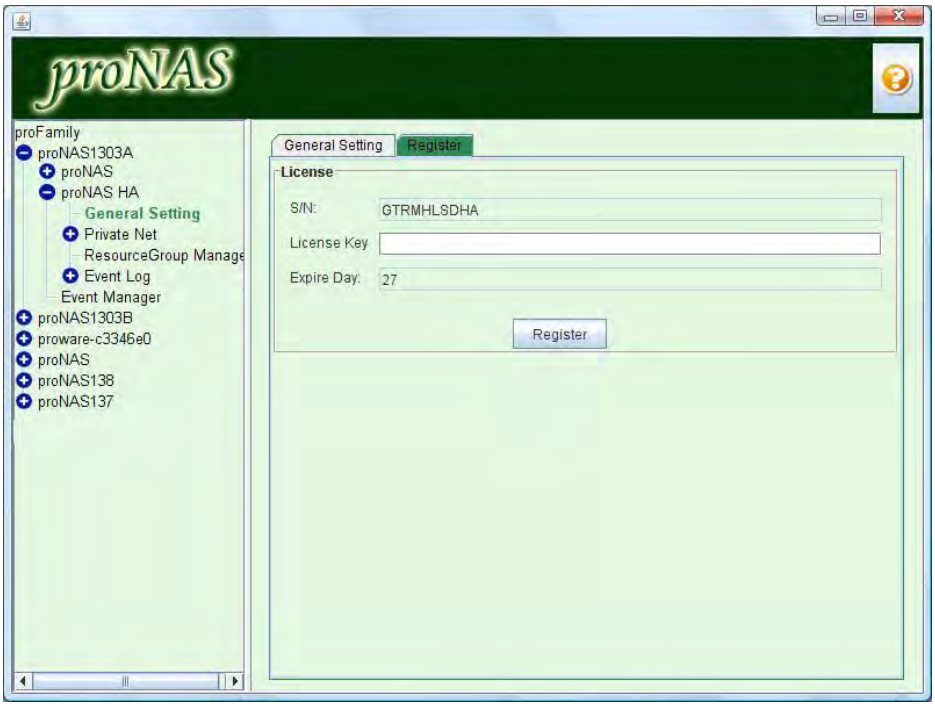
Example of Replication Status after selecting "**No**" to retain all Replication:



All Logical Volume Replication are enabled (Rep. Enable shows "Yes")

8.6 License Registration

To apply ProNAS HA license codes and register them to ProNAS HA, users must first get the S/N of the two servers. Forward the S/N to your local ProNAS HA provider. Then Input the acquired License and click “Register” button. Users can now put ProNAS HA to work.



NOTE: There is a 30-day trial period which users can try. Users must register the HA License within the trial period in order for proNAS HA to continue its function even after the trial period.

8.7 Event Log Properties

All the messages generated by ProNAS HA will be displayed in the Event Log. The messages can help users to identify the possible reasons that prevent ProNAS HA from operating normally.

proNAS
proFamily
proNAS1303A
proNAS
proNAS HA
General Setting
Private Net
ResourceGroup Manage
Event Log
Event Log History
Event Manager
proNAS1303B
proware-c3346e0
proNAS
proNAS138
proNAS137
Event Log
Date
Time
Level
2010/12/20 09:45:36 Warning [005]The proNAS HA will be expired within 27 days, ple
2010/12/20 09:45:36 Normal [727]proNAS HA version:7.0, installed path:/usr/proNA
2010/12/20 09:45:36 Normal [720]***** proNAS HA Service Running *****
2010/12/20 09:45:35 Warning [710]The peer host name is empty. Please go to "Gen
2010/12/20 09:45:35 Trace config file updated
2010/12/20 09:45:35 Trace set logger ok
2010/12/20 09:24:22 Normal [722]----- Cluster Function Stopped -----
2010/12/20 09:24:22 Warning [125]All instances of private net are down or unavailab
2010/12/20 09:24:22 Normal [160]Disable private net [Socket - 172.16.0.11] : Succe
2010/12/20 09:09:39 Error [592]The peer server bring in resource group [RES] : F
2010/12/20 09:09:34 Normal [360]Add resource [IP_RES] : Success.
2010/12/20 09:08:54 Normal [560]Add resource group [RES] : Success.
2010/12/20 09:07:56 Normal Volume Replication: local ip=172.16.0.11, peer host=p
2010/12/20 09:07:10 Normal [721]----- Cluster Function Running -----
2010/12/20 09:07:07 Normal [150]Enable private net [Socket - 172.16.0.11] : Succes
2010/12/20 09:07:05 Warning [100]An error has occurred while initiating private net(T
2010/12/20 09:07:04 Warning [100]An error has occurred while initiating private net(T
2010/12/20 09:05:17 Normal [729]Receive the peer IP information ok.
Refresh